

Dominion LX

Benutzerhandbuch

Version 2.4.5

LX-v2.4.5-0A-G

Oktober 2011

255-80-8009-00

Einhaltung der FCC-Bestimmungen

In Tests wurde festgestellt, dass das Gerät die Grenzwerte für digitale Geräte der Klasse A gemäß Teil 15 der FCC-Bestimmungen einhält. Diese Grenzwerte sollen in kommerziell genutzten Umgebungen einen angemessenen Schutz vor Störungen bieten. Das in diesem Handbuch beschriebene Gerät erzeugt, verbraucht und gibt unter Umständen hochfrequente Strahlung ab und kann bei unsachgemäßer Installation und Verwendung zu Störungen des Rundfunk- und Fernsehempfangs führen. Der Betrieb dieses Geräts in Wohnumgebungen führt unter Umständen zu schädlichen Störungen.

VCCI-Informationen (Japan)

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Raritan ist nicht verantwortlich für Schäden an diesem Produkt, die durch einen Unfall, ein Missgeschick, durch Missbrauch, Fremdeingriffe am Produkt oder andere Ereignisse entstanden sind, die sich außerhalb der Kontrolle von Raritan befinden oder unter normalen Betriebsbedingungen nicht auftreten.



Sicherheitsrichtlinien zur Montage im Serverschrank

Bei Raritan-Produkten, die in ein Gestell montiert werden, sind folgende Vorsichtsmaßnahmen zu beachten:

- Die Betriebstemperatur in einer geschlossenen Gestellumgebung kann höher sein als die Raumtemperatur. Sorgen Sie dafür, dass die für die Appliances angegebene, maximale Umgebungstemperatur nicht überschritten wird. Siehe **Specifications** (Technische Daten).
- Sorgen Sie für eine ausreichende Luftzirkulation in der Gestellumgebung.
- Montieren Sie Geräte im Gestell sorgfältig, um eine ungleichmäßige mechanische Belastung zu vermeiden.
- Schließen Sie die Geräte mit Vorsicht an das Stromnetz an, um eine Überlastung der Stromkreise zu vermeiden.
- Erden Sie alle Geräte ordnungsgemäß, besonders die Anschlüsse an den Netzstromkreis (z. B. Mehrfachsteckdosen statt direkter Anschlüsse).

Inhalt










Raritan.



Kapitel 1 Einleitung

In diesem Kapitel



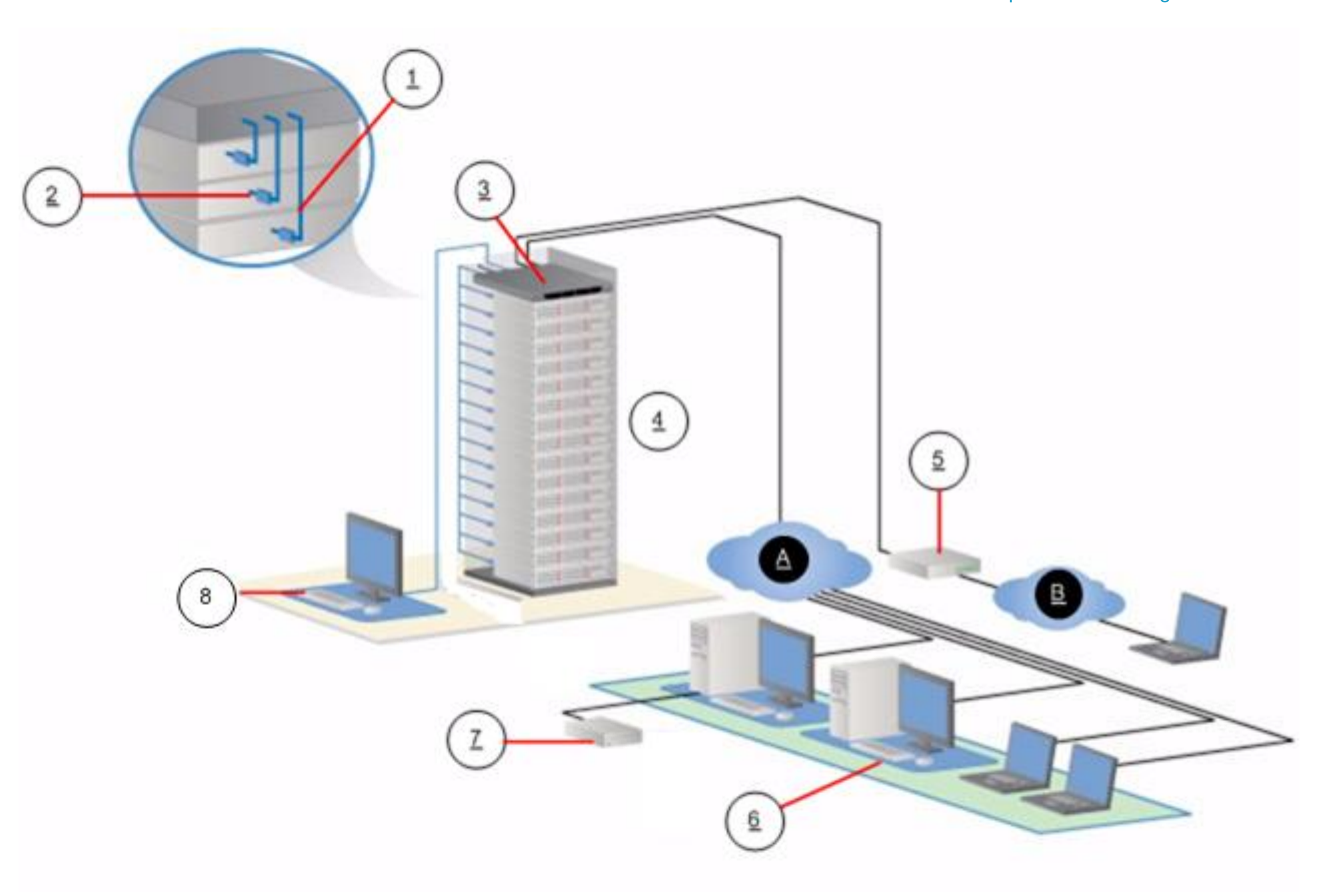
Überblick über LX

Die LX® KVM-über-IP-Switches geben einen an zwei Remotebenutzer, wobei ein unabhängiger lokaler Port, Zugriff auf BIOS-Ebene und die Steuerung von bis zu 16 Servern verfügbar sind. Durch die Implementierung der Schichtfunktion können Benutzer problemlos bis zu 256 Computer von einer einzigen Konsole aus steuern. Diese Anwendungen, die speziell für kleine und mittelständische Unternehmen (KMUs) entwickelt wurden, bieten einen ökonomischen Remotezugriff von jedem beliebigen Standort aus, eine effiziente und zuverlässige Serververwaltung und minimale Startinvestitionen für preisgünstige Skalierbarkeit.

LX ist standardmäßig mit Universal Virtual Media™ von Raritan ausgestattet, wodurch eine Vielzahl von CD-, DVD-, USB-, internen und Remotelaufwerken verfügbar sind, die lokal gemountet werden können und Remoteverwaltungsaufgaben ermöglichen. Dadurch ist es nicht mehr notwendig, dass Sie vor Ort sind. Um Ihnen klare und scharfe Bilder bieten zu können, unterstützt die moderne Architekturplattform die Remote-Videoauflösung in High Definition (HD) von 1920x1080. Darüber hinaus erfordert die allgemeine, grafische browserbasierte Benutzeroberfläche für den lokalen und Remotezugriff nur wenige Kenntnisse, ermöglicht Produktivität am Serverschrank und sorgt für einen effizienten Einsatz aller IT-Ressourcen. Auf die Server kann von Windows®, Linux®, Sun® oder Macintosh® aus über die gängigen Browser oder eigenständig ohne Client-Lizenzgebühren zugegriffen werden.

Durch Kabelbündeloptionen kann das IT-Personal in KMU-Unternehmen die Startinvestitionen zum jetzigen Zeitpunkt minimieren und dabei gleichzeitig die Möglichkeit für zusätzliche Funktionen zu einem späteren Zeitpunkt offenhalten.





Diagrammschlüssel			
1	Kabel der Kategorie 5	6	Remotezugriff (Netzwerk)
2	Computer Interface Module (CIM)	7	Lokaler Zugriff
3	LX	A	IP LAN/WAN
4	Remote-KVM und serielle Remotegeräte	B	PSTN
5	Modem		



Fotos von LX





LX 108


Raritan
Dominion LX-116


MODEM
RESET
LAN

LX 116


Raritan
Dominion LX-216


MODEM
RESET
LAN

LX 216








Raritan.

Paketinhalt

Jedes LX wird als vollständig konfiguriertes, eigenständiges Produkt in einem standardmäßigen 1U-19-Zoll-Gestellchassis geliefert. Im Lieferumfang aller LX-Geräte ist Folgendes enthalten:

Enthaltene Menge	Element
1	LX-Gerät
1	Gestellmontagekit
1	Netzkabel
1	LX-Kurzanleitung
1	Anwendungshinweis
1	Garantiekarte

LX-Client-Anwendungen

Die folgenden Client-Anwendungen können mit LX verwendet werden:

Produkt	Arbeitet mit...				
	MPC	RRC	VKC	RSC	AKC
LX 2.4.5 (oder höher)	✓		✓		✓

Weitere Informationen zu den Client-Anwendungen finden Sie im Benutzerhandbuch **KVM and Serial Client Guide**. Darüber hinaus finden Sie im Abschnitt ***Arbeiten mit Zielservern*** (auf Seite 42) dieses Handbuchs Informationen zur Verwendung von Clients zusammen mit LX.

Hinweis: MPC und VKC benötigen Java™ Runtime Environment (JRE™). Der AKC ist .NET-basiert.

Hardware

- Integrierter KVM-über-IP-Remotezugriff
- Modelle mit 8 und 16 Serverports
- Bis zu zwei Videokanäle, über die bis zu zwei Benutzer gleichzeitig eine Verbindung zu LX herstellen können
- Kapazität für mehrere Benutzer (1/2 Remotebenutzer, 1 lokaler Benutzer)
- UTP-Serverkabel (Kategorie 5/5e/6)
- Ethernet-Port (10/100/1000 LAN)
- Während des Betriebs aufrüstbar
- Lokaler Benutzerport für den Serverschrankzugriff
    - Drei USB 2.0-Ports an der Rückseite für unterstützte USB-Geräte
    - Simultane Reaktion bei Remotebenutzerzugriff
    - Lokale grafische Benutzeroberfläche (GUI) für die Verwaltung
- Modemunterstützung
- LED-Anzeigen an der Vorder- und Rückseite für den Gerätestatus, den Hochfahrvorgang und Firmwareaktualisierungen
- Taste zum Zurücksetzen der Hardware
- Serieller Port zur Verbindung mit einem externen Modem
- 19"-Einschub (Halterungen im Lieferumfang enthalten)



Software

- Unterstützung virtueller Medien in Windows®-, Mac®- und Linux®-Umgebungen mit D2CIM-VUSB und D2CIM-DVUSB CIMs
- Port-Scanfunktion und Miniaturansicht von Zielen innerhalb eines konfigurierbaren Scan-Satzes
- "Absolute Mouse Synchronization" (Absolute Maussynchronisierung) mit den CIMs D2CIM-VUSB und D2CIM-DVUSB
- Plug-and-Play
- Webbasierte(r) Zugriff und Verwaltung
- Intuitive grafische Benutzeroberfläche (GUI)
- 256-Bit-Verschlüsselung des gesamten KVM-Signals, einschließlich Video und virtueller Medien
- LDAP-, Active Directory®-, RADIUS- oder interne Authentifizierung und Autorisierung
- DHCP oder feste IP-Adressen
- SNMP- und Syslog-Verwaltung
- Unterstützung von IPv4 und IPv6
- LX und generische Schichten

LX-Hilfe

Die LX-Hilfe enthält Informationen zur Installation, Einrichtung und Konfiguration des LX. Sie enthält ebenfalls Informationen zum Zugriff auf Zielserver, zur Verwendung von virtuellen Medien, zur Verwaltung von Benutzern und Sicherheit sowie zur Wartung und Diagnose von Problemen des LX.

Weitere Informationen und wichtige Hinweise zur aktuellen Version entnehmen Sie vor der Verwendung von LX den LX-Versionshinweisen.

Eine PDF-Version des Hilfedokuments kann von der Seite **Firmware- und Dokumentationsseite von Raritan** auf der Raritan-Website heruntergeladen werden. Besuchen Sie die Raritan-Website, um die jeweils neuesten Benutzerhandbücher einzusehen.

Um die Online-Hilfe zu verwenden, muss die Option "Active Content" (Aktive Inhalte) Ihres Browsers aktiviert sein. Wenn Sie den Internet Explorer 7 verwenden, müssen Sie "Scriptlets" aktivieren. Informationen zur Aktivierung dieser Funktionen finden Sie in der Hilfe Ihres Browsers.



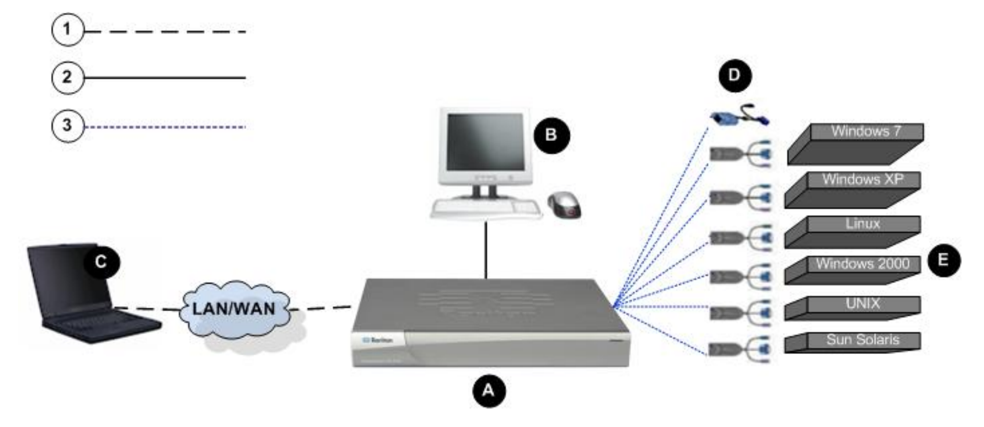
Verwandte Dokumentation

Zur LX-Hilfe gehört auch eine LX-Kurzanleitung, die Sie auf der **Firmware- und Dokumentationsseite von Raritan** auf der ***Raritan-Website*** (***http://www.raritan.com/support/firmware-and-documentation***) finden.

Installationsanforderungen und -anweisungen für Client-Anwendungen, die mit <ProductName< verwendet werden, finden Sie im Benutzerhandbuch **KVM and Serial Access Clients Guide**, welches ebenso auf der Raritan-Website verfügbar ist. Spezifische Client-Funktionen, die mit LX verwendet werden, finden Sie in der Hilfe.

Terminologie

In der Hilfe wird die folgende Terminologie für typische LX-Komponenten verwendet:





Diagrammschlüssel	
1	TCP/IP IPv4 und/oder IPv6 hinzugefügt
2	KVM (Tastatur, Video, Maus)
3	UTP-Kabel (Kat. 5/5e/6)
A	LX
B	Lokale Zugriffskonsole Lokaler Benutzer – eine optionale, direkt mit LX verbundene Benutzerkonsole (bestehend aus Tastatur, Maus und MultiSync-VGA-Monitor) für die Steuerung der KVM-Zielserver (direkt am Gestell, nicht über das Netzwerk).
C	Remote-PC Vernetzte Computer für den Zugriff auf die mit LX verbundenen KVM-Zielserver und deren Steuerung.
D	CIMs Dongles, die eine Verbindung mit jedem Zielserver herstellen. Für alle unterstützten Betriebssysteme verfügbar
E	Zielserver KVM-Zielserver – Server mit Videokarten und Benutzeroberflächen (z. B. Windows®, Linux®, Solaris™ usw.), auf die über LX von einem Remotestandort aus zugegriffen wird.

Eine Liste der unterstützten Betriebssysteme und CIMs finden Sie unter Unterstützte CIMs und Betriebssysteme – LX.

Kapitel 2 Installation und Konfiguration

In diesem Kapitel

Überblick

Dieser Abschnitt enthält einen kurzen Überblick über den Installationsprozess. Die einzelnen Schritte werden im Verlauf des Kapitels noch genauer erläutert.

So installieren und konfigurieren Sie LX:

- ***Schritt 1: Konfigurieren der KVM-Zielserver*** (siehe "***Schritt 1: Konfigurieren der KVM-Zielserver***" auf Seite 13)
- ***Schritt 2: Konfigurieren der Einstellungen für die Netzwerkfirewall*** (siehe "***Schritt 2: Konfigurieren der Einstellungen für die Netzwerkfirewall***" auf Seite 29)
- ***Schritt 3: Anschließen der Geräte*** (siehe "***Schritt 3: Anschließen der Geräte***" auf Seite 30)
- ***Schritt 4: Konfigurieren von LX*** (siehe "***Schritt 4: Konfigurieren von LX***" auf Seite 33)
- ***Schritt 5: Starten der LX-Remotekonsole*** (siehe "***Schritt 5: Starten der LX-Remotekonsole***" auf Seite 38)
- ***Schritt 6: Konfigurieren der Tastatursprache (optional)*** (siehe "***Schritt 6: Konfigurieren der Tastatursprache (optional)***" auf Seite 40)
- ***Schritt 7: Konfigurieren von Schichten (optional)*** (siehe "***Schritt 7: Konfigurieren von Schichten (optional)***" auf Seite 41)

Dieser Abschnitt enthält außerdem die erforderlichen Informationen zur Standardanmeldung. Dazu zählen die Standard-IP-Adresse, der Standardbenutzername und das Standardkennwort. Siehe ***Standard-Anmeldeinformationen*** (auf Seite 12).

Standard-Anmeldeinformationen

Standard	Wert
Benutzername	Der Standardbenutzername ist "admin". Dieser Benutzer besitzt Administratorrechte.
Kennwort	Das Standardkennwort ist "raritan".

Standard	Wert
	Kennwörter unterliegen der Groß-/Kleinschreibung und müssen genau in der bei ihrer Erstellung verwendeten Schreibweise eingegeben werden. Das Standardkennwort "raritan" beispielsweise muss in Kleinbuchstaben eingegeben werden. Beim ersten Starten des LX müssen Sie das Standardkennwort ändern.
IP-Adresse	LX wird mit der Standard-IP-Adresse 192.168.0.192 geliefert.

Wichtig: Für die Sicherung und zur Gewährleistung der Geschäftskontinuität sollten Sie unbedingt einen Benutzernamen und ein Kennwort für den Sicherungsadministrator erstellen und diese Informationen an einem sicheren Ort aufbewahren.

Erste Schritte

Schritt 1: Konfigurieren der KVM-Zielserver

KVM-Zielserver sind die Computer, auf die über LX zugegriffen wird und die von diesem aus gesteuert werden. Konfigurieren Sie vor der Installation des LX alle KVM-Zielserver, um eine optimale Leistung sicherzustellen. Diese Konfiguration gilt nur für KVM-Zielserver, nicht jedoch für Clientworkstations (Remote-PCs), die für den Remotezugriff auf LX verwendet werden.

Desktop-Hintergrund

Verwenden Sie für eine optimale Bandbreiteneffizienz und Videoleistung nach Möglichkeit einen einfarbigen Hintergrund. Hintergrundbilder mit Fotos oder komplexen Farbverläufen können die Leistung beeinträchtigen.

Unterstützte Videoauflösungen

Stellen Sie sicher, dass die Videoauflösung und die Aktualisierungsfrequenz aller Zielserver von LX unterstützt werden und das Signal keinen Zeilensprung beinhaltet.

Die Videoauflösung und die Kabellänge sind wichtige Faktoren für die Maussynchronisierung. Siehe ***Verbindungsentfernung zum Zielserver und Videoauflösung*** (auf Seite 232).

Die folgenden Auflösungen werden von LX unterstützt:

Auflösungen	
640 x 350 bei 70Hz	1024 x 768 bei 85Hz
640 x 350 bei 85Hz	1024 x 768 bei 75Hz
640 x 400 bei 56Hz	1024 x 768 bei 90Hz
640 x 400 bei 84Hz	1024 x 768 bei 100Hz
640 x 400 bei 85Hz	1152 x 864 bei 60Hz
640 x 480 bei 60Hz	1152 x 864 bei 70Hz
640 x 480 bei 66,6Hz	1152 x 864 bei 75Hz
640 x 480 bei 72Hz	1152 x 864 bei 85Hz
640 x 480 bei 75Hz	1.152 x 870 bei 75,1Hz
640 x 480 bei 85Hz	1.152 x 900 bei 66Hz
720 x 400 bei 70Hz	1.152 x 900 bei 76Hz
720 x 400 bei 84Hz	1.280 x 720 bei 60Hz
720 x 400 bei 85Hz	1.280 x 960 bei 60Hz
800 x 600 bei 56Hz	1.280 x 960 bei 85Hz
800 x 600 bei 60Hz	1280 x 1024 bei 60Hz
800 x 600 bei 70Hz	1280 x 1024 bei 75Hz
800 x 600 bei 72Hz	1280 x 1024 bei 85Hz
800 x 600 bei 75Hz	1.360 x 768 bei 60Hz
800 x 600 bei 85Hz	1.366 x 768 bei 60Hz
800 x 600 bei 90Hz	1.368 x 768 bei 60Hz
800 x 600 bei 100Hz	1.400 x 1050 bei 60Hz
832 x 624 bei 75,1Hz	1.440 x 900 bei 60Hz
1024 x 768 bei 60Hz	1600 x 1200 bei 60Hz



Auflösungen	
1024 x 768 bei 70Hz	1.680 x 1.050 bei 60Hz
1024 x 768 bei 72Hz	1920 x 1080 bei 60Hz

Mausmodi

LX arbeitet in den Mausmodi "Absolute" (Absolut)™, "Intelligent" (Intelligent) und "Standard" (Standard).

Für den Mausmodus "Absolute Mouse Synchronization" (Absolute Maussynchronisierung) müssen die Mausparameter nicht geändert werden. Es ist jedoch ein D2CIM-VUSB oder ein D2CIM-DVUSB erforderlich. In den Mausmodi "Standard" und "Intelligent" müssen die Mausparameter auf bestimmte Werte festgelegt werden. Mauskonfigurationen variieren je nach Ziel-Betriebssystem. Weitere Informationen finden Sie in der Dokumentation für Ihr Betriebssystem.

Der "Intelligent Mouse Mode" (Intelligente Mausmodus) funktioniert auf den meisten Windows-Plattformen, er kann jedoch zu unvorhersehbaren Ergebnissen führen, wenn auf dem Zielgerät der Active Desktop aktiviert ist. Verwenden Sie im "Intelligent Mouse Mode" (Intelligenten Mausmodus) keinen animierten Cursor.

Einstellungen für Windows XP, Windows 2003 und Windows 2008

▶ So konfigurieren Sie KVM-Zielserver, auf denen die Betriebssysteme Microsoft ® Windows XP®, Windows 2003® oder Windows 2008® ausgeführt werden:

1. Konfigurieren der Mauseinstellungen:
   a. Wählen Sie "Start" > "Systemsteuerung" > "Maus" aus.
   b. Klicken Sie auf die Registerkarte "Zeigeroptionen".
   c. Führen Sie im Bereich "Bewegung" folgende Schritte aus:

- Stellen Sie die Mausgeschwindigkeit genau auf die mittlere Geschwindigkeitseinstellung ein.
- Deaktivieren Sie die Option "Enhance pointer precision" (Zeigerbeschleunigung verbessern).
- Deaktivieren Sie die Option "Zur Standardschaltfläche springen".
- Klicken Sie auf "OK".

Hinweis: Wenn Sie Windows 2003 auf Ihrem Zielserver ausführen, über KVM auf den Server zugreifen und eine der unten aufgelisteten Aktionen durchführen, kann die Maussynchronisierung deaktiviert werden, wenn diese zuvor aktiviert war. In diesem Fall müssen Sie im Client-Menü "Mouse" (Maus) den Befehl "Synchronize Mouse" (Maus synchronisieren) auswählen, um sie erneut zu aktivieren. Im Folgenden werden die Aktionen aufgelistet, die zur Deaktivierung der Maussynchronisierung führen können:

- Öffnen eines Texteditors

- Zugreifen auf die Maus- oder Tastatureigenschaften sowie Telefon- und Modusoptionen über die Windows-Systemsteuerung.

---

2. Deaktivieren Sie die Übergangseffekte:
   a. Wählen Sie in der Systemsteuerung die Option "Anzeige" aus.
   b. Klicken Sie auf die Registerkarte "Darstellung".
   c. Klicken Sie auf "Effekte".
   d. Deaktivieren Sie das Kontrollkästchen "Folgende Übergangseffekte für Menüs und QuickInfos verwenden".
   e. Klicken Sie auf "OK".
3. Schließen Sie die Systemsteuerung.



Hinweis: Für KVM-Zielserver, auf denen Windows XP, Windows 2000 oder Windows 2008 ausgeführt wird, können Sie einen Benutzernamen erstellen, der nur für Remoteverbindungen über LX verwendet wird. Auf diese Weise können Sie die langsamen Einstellungen für die Mausgeschwindigkeit/-beschleunigung auf die LX-Verbindung beschränken.

Die Anmeldeseiten von Windows XP, Windows 2000 und Windows 2008 werden auf die voreingestellten Mausparameter zurückgesetzt. Diese Einstellungen unterscheiden sich von den für eine optimale Leistung von LX empfohlenen Einstellungen. Daher ist bei diesen Bildschirmen die Maussynchronisation möglicherweise nicht optimal.

Hinweis: Fahren Sie nur fort, wenn Sie sich mit dem Anpassen der Registrierung von Windows-KVM-Zielservern auskennen. Sie können auf den Anmeldeseiten eine bessere LX-Maussynchronisierung erzielen, indem Sie hierzu mit dem Registrierungseditor von Windows die folgenden Einstellungen ändern: HKey_USERS\.DEFAULT\Systemsteuerung\Maus: > MouseSpeed = 0;MouseThreshold 1=0;MouseThreshold 2=0.

Einstellungen für Windows 7 und Windows Vista

So konfigurieren Sie KVM-Zielserver, auf denen Windows Vista® ausgeführt wird:

1. Konfigurieren der Mauseinstellungen:
   a. Wählen Sie **Start > Einstellungen > Systemsteuerung > Maus**.
   b. Wählen Sie "Erweiterte Systemeinstellungen" im linken Navigationsfenster aus. Das Dialogfeld "Systemeigenschaften" wird angezeigt.
   c. Klicken Sie auf die Registerkarte "Zeigeroptionen".
   d. Führen Sie im Bereich "Bewegung" folgende Schritte aus:
      - Stellen Sie die Mausgeschwindigkeit genau auf die mittlere Geschwindigkeitseinstellung ein.
      - Deaktivieren Sie das Kontrollkästchen "Zeigerbeschleunigung verbessern".
      - Klicken Sie auf "OK".
2. Deaktivieren Sie die Animations- und Einblendeffekte:
   a. Wählen Sie in der Systemsteuerung die Option "System".
   b. Wählen Sie "Leistungsinformationen" und anschließend "Tools" > "Weitere Tools" > "Darstellung und Leistung von Windows anpassen" aus.
   c. Klicken Sie auf die Registerkarte "Erweitert".



d. Klicken Sie in der Gruppe "Leistung" auf die Schaltfläche "Einstellungen", um das Dialogfeld "Leistungsoptionen" zu öffnen.

e. Deaktivieren Sie im Bereich "Benutzerdefiniert" die folgenden Kontrollkästchen:

- Animationsoptionen:
  - Steuerelemente und Elemente innerhalb von Fenstern animieren
  - Animation beim Minimieren und Maximieren von Fenstern
- Einblendoptionen:
  - Menüs in Ansicht ein- oder ausblenden
  - Quickinfo in Ansicht ein- oder ausblenden
  - Menüelemente nach Aufruf ausblenden

3. Klicken Sie auf "OK", und schließen Sie die Systemsteuerung.

So konfigurieren Sie KVM-Zielserver, auf denen Windows 7® ausgeführt wird:

1. Konfigurieren der Mauseinstellungen:

   a. Wählen Sie "Start" > "Systemsteuerung" > "Hardware und Sound" > "Maus" aus.

   b. Klicken Sie auf die Registerkarte "Zeigeroptionen".

   c. Führen Sie im Bereich "Bewegung" folgende Schritte aus:

   - Stellen Sie die Mausgeschwindigkeit genau auf die mittlere Geschwindigkeitseinstellung ein.
   - Deaktivieren Sie das Kontrollkästchen "Zeigerbeschleunigung verbessern".
   - Klicken Sie auf OK.

2. Deaktivieren der Animations- und Einblendeffekte:

   a. Wählen Sie "Systemsteuerung" > "System und Sicherheit" aus.

   b. Wählen Sie "System" und anschließend "Erweiterte Systemeinstellungen" im linken Navigationsfenster aus. Das Dialogfeld "Systemeigenschaften" wird angezeigt.

   c. Klicken Sie auf die Registerkarte "Erweitert".

   d. Klicken Sie in der Gruppe "Performance" (Leistung) auf die Schaltfläche "Settings" (Einstellungen), um das Dialogfeld "Performance Options" (Leistungsoptionen) zu öffnen.

   e. Deaktivieren Sie im Bereich "Benutzerdefiniert" die folgenden Kontrollkästchen:



- Animationsoptionen:
  - Steuerelemente und Elemente innerhalb von Fenstern animieren
  - Animation beim Minimieren und Maximieren von Fenstern
- Einblendoptionen:
  - Menüs in Ansicht ein- oder ausblenden
  - QuickInfo in Ansicht ein- oder ausblenden
  - Menüelemente nach Aufruf ausblenden

3. Klicken Sie auf "OK", und schließen Sie die Systemsteuerung.

Einstellungen für Windows 2000

▶ So konfigurieren Sie KVM-Zielserver, auf denen Microsoft® Windows 2000® ausgeführt wird:

1. Konfigurieren der Mauseinstellungen:
   a. Wählen Sie "Start" > "Systemsteuerung" > "Maus" aus.
   b. Öffnen Sie die Registerkarte "Motion" (Bewegung).
      - Stellen Sie die Beschleunigung auf "Keine" ein.
      - Stellen Sie die Mausgeschwindigkeit genau auf die mittlere Geschwindigkeitseinstellung ein.
      - Klicken Sie auf OK.
2. Deaktivieren der Übergangseffekte:
   a. Wählen Sie in der Systemsteuerung die Option "Anzeige" aus.
   b. Klicken Sie auf die Registerkarte "Effekte".
      - Deaktivieren Sie das Kontrollkästchen "Folgende Übergangseffekte für Menüs und QuickInfos verwenden".
3. Klicken Sie auf "OK", und schließen Sie die Systemsteuerung.

Hinweis: Für KVM-Zielserver, auf denen Windows XP, Windows 2000 oder Windows 2008 ausgeführt wird, können Sie einen Benutzernamen erstellen, der nur für Remoteverbindungen über LX verwendet wird. Auf diese Weise können Sie die langsamen Einstellungen für die Mausgeschwindigkeit/-beschleunigung auf die LX-Verbindung beschränken.

Die Anmeldeseiten von Windows XP, Windows 2000 und Windows 2008 werden auf die voreingestellten Mausparameter zurückgesetzt. Diese Einstellungen unterscheiden sich von den für eine optimale Leistung von LX empfohlenen Einstellungen. Daher ist bei diesen Bildschirmen die Maussynchronisation möglicherweise nicht optimal.

Hinweis: Fahren Sie nur fort, wenn Sie sich mit dem Anpassen der Registrierung von Windows-KVM-Zielservern auskennen. Sie können auf den Anmeldeseiten eine bessere LX-Maussynchronisierung erzielen, indem Sie hierzu mit dem Registrierungseditor von Windows die folgenden Einstellungen ändern: HKey_USERS\.DEFAULT\Systemsteuerung\Maus: > MouseSpeed = 0;MouseThreshold 1=0;MouseThreshold 2=0.

Einstellungen für Linux (Red Hat 9)

Hinweis: Die folgenden Einstellungen sind nur für den Mausmodus "Standard" optimiert.

▶ So konfigurieren Sie KVM-Zielserver, auf denen Linux® ausgeführt wird (grafische Benutzeroberfläche):

1. Konfigurieren der Mauseinstellungen:
   a. Wählen Sie "Main Menu" > "Preferences" > "Mouse" (Hauptmenü > Einstellungen > Maus) aus. Das Dialogfeld "Mouse Preferences" (Mauseinstellungen) wird angezeigt.
   b. Öffnen Sie die Registerkarte "Motion" (Bewegung).
   c. Stellen Sie in der Gruppe "Speed" (Geschwindigkeit) den Beschleunigungsregler genau auf die mittlere Position ein.
   d. Stellen Sie in der Gruppe "Speed" (Geschwindigkeit) die Sensibilität auf niedrig ein.
   e. Stellen Sie in der Gruppe "Drag & Drop" (Ziehen & Ablegen) den Grenzwert auf niedrig ein.
   f. Schließen Sie das Dialogfeld "Mouse Preferences" (Mauseinstellungen).

   Hinweis: Wenn diese Schritte nicht den gewünschten Erfolg erzielen, geben Sie den Befehl "xset mouse 1 1" wie in den Kommandozeilenanweisungen für Linux beschrieben aus.

2. Konfigurieren der Bildschirmauflösung:



a. Wählen Sie "Main Menu" > "System Settings" > "Display" (Hauptmenü > Systemeinstellungen > Anzeige) aus. Das Dialogfeld "Display Settings" (Anzeigeeinstellungen) wird angezeigt.

b. Wählen Sie auf der Registerkarte "Display" (Anzeige) eine Auflösung aus, die von LX unterstützt wird.

c. Überprüfen Sie auf der Registerkarte "Advanced" (Erweitert), dass die Aktualisierungsfrequenz von LX unterstützt wird.

Hinweis: Wenn eine Verbindung zum Zielserver hergestellt ist, wird bei vielen grafischen Linux-Umgebungen durch den Befehl "<Strg> <Alt> <+>" die Videoauflösung geändert, indem ein Bildlauf durch alle verfügbaren (noch aktivierten) Auflösungen in der Datei "XF86Config" oder "/etc/X11/xorg.conf" (je nach X-Server-Distribution) durchgeführt wird.

So konfigurieren Sie KVM-Zielserver, auf denen Linux ausgeführt wird (Kommandozeile):

1. Stellen Sie die Mausbeschleunigung und den Grenzwert genau auf 1 ein. Geben Sie folgenden Befehl ein: *xset mouse 1 1*. Die Einstellung sollte bei der Anmeldung übernommen werden.
2. Stellen Sie sicher, dass jeder Linux-Zielserver eine von LX unterstützte Auflösung mit einer standardmäßigen VESA-Auflösung und Aktualisierungsfrequenz verwendet.
3. Jeder Linux-Zielserver sollte außerdem so eingestellt sein, dass sich die Deaktivierungszeiten im Bereich von ±40 % der VESA-Standardwerte bewegen.

    a. Rufen Sie die Xfree86-Konfigurationsdatei "XF86Config" auf.

    b. Deaktivieren Sie mithilfe eines Texteditors alle nicht von LX unterstützten Auflösungen.

    c. Deaktivieren Sie die virtuelle Desktop-Funktion, (nicht von LX unterstützt).

    d. Prüfen Sie die Deaktivierungszeiten (±40 % der VESA-Standardwerte).

    e. Starten Sie den Computer neu.

Hinweis: Wenn Sie die Videoauflösung ändern, müssen Sie sich vom Zielserver abmelden und anschließend wieder anmelden, damit die Videoeinstellungen wirksam werden.

Hinweis für Red Hat 9-KVM-Zielserver

Wenn auf dem Zielserver Red Hat® 9 unter Verwendung eines USB-CIM ausgeführt wird und Probleme mit der Tastatur und/oder der Maus auftreten, können Sie eine zusätzliche Konfigurationseinstellung vornehmen.

Tipp: Sie müssen diese Schritte ggf. auch nach der Installation eines Betriebssystems durchführen.

So konfigurieren Sie Red Hat 9-Server mit USB-CIMs:

1. Navigieren Sie zur Konfigurationsdatei Ihres Systems (in der Regel /etc/modules.conf).
2. Verwenden Sie einen Editor Ihrer Wahl und stellen Sie sicher, dass die Zeile "alias usb-controller" in der Datei "modules.conf" wie folgt lautet:

   alias usb-controller usb-uhci

   Hinweis: Wenn die Datei "/etc/modules.conf" bereits eine andere Zeile mit "usb-uhci" enthält, muss die Zeile entfernt oder auskommentiert werden.

   ---

3. Speichern Sie die Datei.
4. Starten Sie das System neu, um die Änderungen zu übernehmen.

Einstellungen für Linux (Red Hat 4)

Hinweis: Die folgenden Einstellungen sind nur für den Mausmodus "Standard" optimiert.

So konfigurieren Sie KVM-Zielserver, auf denen Linux® ausgeführt wird (grafische Benutzeroberfläche):

1. Konfigurieren der Mauseinstellungen:
   a. Red Hat 5-Benutzer: Wählen Sie "Main Menu" > "Preferences" > "Mouse" (Hauptmenü > Einstellungen > Maus) aus. Red Hat 4-Benutzer: Wählen Sie "System" > "Preferences" > "Mouse" (System > Einstellungen > Maus) aus. Das Dialogfeld "Mouse Preferences" (Mauseinstellungen) wird angezeigt.
   b. Klicken Sie auf die Registerkarte "Motion" (Bewegung).
   c. Stellen Sie in der Gruppe "Speed" (Geschwindigkeit) den Beschleunigungsregler genau auf die mittlere Position ein.



d. Stellen Sie in der Gruppe "Speed" (Geschwindigkeit) die Sensibilität auf niedrig ein.

e. Stellen Sie in der Gruppe "Drag & Drop" (Ziehen & Ablegen) den Grenzwert auf niedrig ein.

f. Schließen Sie das Dialogfeld "Mouse Preferences" (Mauseinstellungen).

Hinweis: Wenn diese Schritte nicht den gewünschten Erfolg erzielen, geben Sie den Befehl "xset mouse 1 1" wie in den Kommandozeilenanweisungen für Linux beschrieben aus.

2. Konfigurieren der Bildschirmauflösung:

   a. Wählen Sie "Main Menu" > "System Settings" > "Display" (Hauptmenü > Systemeinstellungen > Anzeige) aus. Das Dialogfeld "Display Settings" (Anzeigeeinstellungen) wird angezeigt.

   b. Wählen Sie auf der Registerkarte "Settings" (Einstellungen) eine Auflösung aus, die von LX unterstützt wird.

   c. Klicken Sie auf OK.

Hinweis: Wenn eine Verbindung zum Zielserver hergestellt ist, wird bei vielen grafischen Linux-Umgebungen durch den Befehl "<Strg> <Alt> <+>" die Videoauflösung geändert, indem ein Bildlauf durch alle verfügbaren (noch aktivierten) Auflösungen in der Datei "XF86Config" oder "/etc/X11/xorg.conf" (je nach X-Server-Distribution) durchgeführt wird.

Hinweis: Wenn Sie die Videoauflösung ändern, müssen Sie sich vom Zielserver abmelden und anschließend wieder anmelden, damit die Videoeinstellungen wirksam werden.

Einstellungen für SUSE Linux 10.1

Hinweis: Versuchen Sie nicht, die Maus bei der SUSE Linux®-Anmeldeaufforderung zu synchronisieren. Sie müssen mit dem Zielserver verbunden sein, um die Cursor zu synchronisieren.

▸ So konfigurieren Sie die Mauseinstellungen:

1. Wählen Sie "Desktop" > "Control Center" (Desktop > Steuerzentrale) aus. Das Dialogfeld "Desktop Preferences" (Desktopeinstellungen) wird angezeigt.
2. Klicken Sie auf "Mouse" (Maus). Das Dialogfeld "Mouse Preferences" (Mauseinstellungen) wird angezeigt.
3. Öffnen Sie die Registerkarte "Motion" (Bewegung).
4. Stellen Sie in der Gruppe "Speed" (Geschwindigkeit) den Beschleunigungsregler genau auf die mittlere Position ein.

5. Stellen Sie in der Gruppe "Speed" (Geschwindigkeit) den Sensibilitätsregler auf niedrig ein.
6. Stellen Sie in der Gruppe "Drag & Drop" (Ziehen & Ablegen) den Grenzwertregler auf niedrig ein.
7. Klicken Sie auf "Close" (Schließen).

So konfigurieren Sie die Videoeinstellungen:

1. Wählen Sie "Desktop Preferences" > "Graphics Card and Monitor" (Desktopeinstellungen > Grafikkarte und Monitor) aus. Das Dialogfeld "Card and Monitor Properties" (Karten- und Monitoreigenschaften) wird angezeigt.
2. Überprüfen Sie, dass eine Auflösung und eine Aktualisierungsfrequenz verwendet werden, die von LX unterstützt werden. Weitere Informationen finden Sie unter **Unterstützte Videoauflösungen**.

   Hinweis: Wenn Sie die Videoauflösung ändern, müssen Sie sich vom Zielserver abmelden und anschließend wieder anmelden, damit die Videoeinstellungen wirksam werden.

Speichern der Linux-Einstellungen

Hinweis: Die Vorgehensweise kann je nach verwendeter Linux®-Version leicht abweichen.

So speichern Sie Ihre Linux-Einstellungen (Aufforderung):

1. Wählen Sie "System Menu" > "Preferences" > "Personal" > "Sessions" (Systemmenü > Einstellungen > Eigene > Sitzungen) aus.
2. Klicken Sie auf die Registerkarte "Session Options" (Sitzungsoptionen).
3. Aktivieren Sie das Kontrollkästchen "Prompt on log off" (Aufforderung bei Abmeldung) und klicken Sie auf OK. Bei dieser Option werden Sie dazu aufgefordert, Ihre aktuelle Sitzung zu speichern, wenn Sie sich abmelden.
4. Wählen Sie bei der Abmeldung im Dialogfeld die Option "Save current setup" (Aktuelle Einstellungen speichern) aus.
5. Klicken Sie auf OK.

Tipp: Wenn Sie nicht bei jeder Abmeldung zum Speichern aufgefordert werden möchten, führen Sie stattdessen die folgenden Schritte durch.

So speichern Sie Ihre Linux-Einstellungen (keine Aufforderung):

1. Wählen Sie "Desktop" > "Control Center" > "System" > "Sessions" (Desktop > Steuerzentrale > System > Sitzungen) aus.

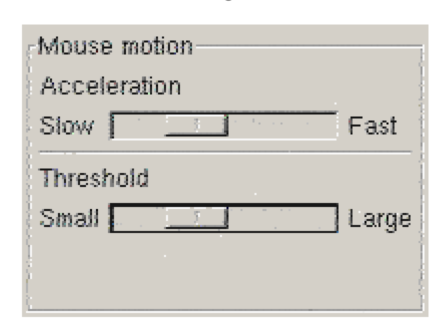


2. Klicken Sie auf die Registerkarte "Session Options" (Sitzungsoptionen).
3. Deaktivieren Sie das Kontrollkästchen "Prompt on the log off" (Aufforderung bei Abmeldung).
4. Aktivieren Sie das Kontrollkästchen "Automatically save changes to the session" (Änderungen der Sitzung automatisch speichern) und klicken Sie auf OK. Bei dieser Option wird Ihre aktuelle Sitzung automatisch gespeichert, wenn Sie sich abmelden.

Einstellungen für Sun Solaris

- **So konfigurieren Sie KVM-Zielserver, auf denen Sun™ Solaris™ ausgeführt wird:**

1. Stellen Sie die Mausbeschleunigung und den Grenzwert genau auf 1 ein. Dies kann über folgende Optionen durchgeführt werden:
   - Über die grafische Benutzeroberfläche.



   - Über die Kommandozeile *xset mouse a t*, wobei *a* die Beschleunigung und *t* der Grenzwert ist.

2. Alle KVM-Zielserver müssen mit einer Anzeigeauflösung konfiguriert werden, die von LX unterstützt wird. Zu den am häufigsten verwendeten unterstützten Auflösungen für Sun-Systeme zählen:

Anzeigeauflösung	Vertikale Aktualisierungsfrequenz	Seitenverhältnis
1600 x 1200	60 Hz	4:3
1280 x 1024	60, 75, 85 Hz	5:4
1152 x 864	75 Hz	4:3
1024 x 768	60, 70, 75, 85 Hz	4:3
800 x 600	56, 60, 72, 75, 85 Hz	4:3
720 x 400	85 Hz	9:5
640 x 480	60, 72, 75, 85 Hz	4:3



3. KVM-Zielserver mit dem Solaris-Betriebssystem müssen eine VGA-Buchse mit TV-Out-Signal haben (mit H- und V-Synchronisierung, keine Composite-Synchronisierung).

So ändern Sie den Sun-Grafikkartenausgang von der Composite-Synchronisierung auf die nicht standardmäßige VGA-Ausgabe:

1. Geben Sie den Befehl "Stop+A" aus, um in den BootProm-Modus zu wechseln.
2. Geben Sie den folgenden Befehl aus, um die Ausgabeauflösung zu ändern: *setenv output-device screen:r1024x768x70*
3. Starten Sie den Server mit dem Befehl `boot` neu.

Sie können sich stattdessen auch an Ihren Raritan-Ansprechpartner wenden und einen Videoausgabeadapter erwerben.

Vorhandene Einstellung	Zu verwendender Videoausgabeadapter
Sun 13W3 mit Composite-Synchronisierungsausgabe	APSSUN II Guardian-Converter
Sun HD15 mit Composite-Synchronisierungsausgabe	1396C-Converter für die Konvertierung von HD15 zu 13W3 und ein APSSUN II Guardian-Converter, der die Composite-Synchronisierung unterstützt
Sun HD15 mit separater Synchronisierungsausgabe	APKMSUN Guardian-Converter

Hinweis: Einige Sun-Hintergrundanzeigen werden möglicherweise auf bestimmten Sun-Servern mit dunklen Rändern nicht exakt zentriert abgebildet. Verwenden Sie einen anderen Hintergrund, oder platzieren Sie oben in der linken Ecke ein helles Symbol.

Mauseinstellungen

So konfigurieren Sie die Mauseinstellungen (Sun Solaris 10.1):

1. Wählen Sie den Launcher aus. Die "Desktop Controls" (Desktopsteuerung) des "Application Manager" (Anwendungsmanager) wird geöffnet.
2. Wählen Sie "Mouse Style Manager" (Mausstilmanager) aus. Das Dialogfeld "Mouse" (Maus) des "Style Manager" (Stilmanager) wird angezeigt.
3. Stellen Sie den Beschleunigungsregler auf 1.0.
4. Stellen Sie den Grenzwertregler auf 1.0.
5. Klicken Sie auf OK.



Aufrufen der Kommandozeile

1. Klicken Sie auf die rechte Maustaste.
2. Wählen Sie "Tools" > "Terminal" (Tools > Endgerät) aus. Ein Terminalfenster wird angezeigt. (Sie sollten sich auf Stammebene befinden, um Befehle auszugeben.)

Videoeinstellungen (POST)

Sun-Systeme verfügen über zwei verschiedene Auflösungseinstellungen: eine POST- und eine GUI-Auflösung. Führen Sie diese Befehle von der Kommandozeile aus durch.

Hinweis: 1024x768x75 wird hier als Beispiel verwendet. Ersetzen Sie das Beispiel durch die Auflösung und Aktualisierungsfrequenz, die Sie verwenden.

So überprüfen Sie die aktuelle POST-Auflösung:

- Führen Sie den folgenden Befehl als Stammbenutzer aus: `# eeprom output-device`

So ändern Sie die POST-Auflösung:

1. Führen Sie `# eeprom output-device=screen:r1024x768x75` aus.
2. Melden Sie sich ab, oder starten Sie den Computer neu.

Videoeinstellungen (GUI)

Die GUI-Auflösung kann je nach verwendeter Grafikkarte mithilfe unterschiedlicher Befehle überprüft und eingestellt werden. Führen Sie diese Befehle von der Kommandozeile aus durch.

Hinweis: 1024x768x75 wird hier als Beispiel verwendet. Ersetzen Sie das Beispiel durch die Auflösung und Aktualisierungsfrequenz, die Sie verwenden.



Karte	Überprüfen der Auflösung durch:	Ändern der Auflösung durch:
32-Bit	# /usr/sbin/pgxconfig -prconf	1. # /usr/sbin/pgxconfig -res 1024x768x75 2. Melden Sie sich ab, oder starten Sie den Computer neu.
64-Bit	# /usr/sbin/m64config -prconf	1. # /usr/sbin/m64config -res 1024x768x75 2. Melden Sie sich ab, oder starten Sie den Computer neu.
32-Bit und 64-Bit	# /usr/sbin/fbconfig -prconf	1. # /usr/sbin/fbconfig -res 1024x768x75 2. Melden Sie sich ab, oder starten Sie den Computer neu.

Einstellungen für IBM AIX 5.3

Führen Sie die folgenden Schritte durch, um KVM-Zielserver zu konfigurieren, auf denen IBM® AIX™ 5.3 ausgeführt wird.

▶ So konfigurieren Sie die Maus:

1. Öffnen Sie den Launcher.
2. Wählen Sie "Style Manager" (Stilmanager) aus.
3. Klicken Sie auf "Mouse" (Maus). Das Dialogfeld "Mouse" (Maus) des "Style Manager" (Stilmanager) wird angezeigt.
4. Stellen Sie mithilfe der Schieberegler die Mausbeschleunigung und den Grenzwert auf 1.0.
5. Klicken Sie auf OK.

▶ So konfigurieren Sie die Videoeinstellungen:

1. Wählen Sie im Launcher "Application Manager" (Anwendungsmanager) aus.
2. Wählen Sie "System_Admin" aus.
3. Wählen Sie "Smit" > "Devices" > "Graphic Displays" > "Select the Display Resolution and Refresh Rate" (Smit > Geräte > Grafische Anzeigen > Anzeigeauflösung und Aktualisierungsfrequenz auswählen) aus.
4. Wählen Sie die verwendete Grafikkarte aus.



5. Klicken Sie auf "List" (Auflisten). Eine Liste der Anzeigemodi wird angezeigt.
6. Wählen Sie eine Auflösung und Aktualisierungsfrequenz aus, die von LX unterstützt wird. Weitere Informationen finden Sie unter Unterstützte Videoauflösungen.

Hinweis: Wenn Sie die Videoauflösung ändern, müssen Sie sich vom Zielserver abmelden und anschließend wieder anmelden, damit die Videoeinstellungen wirksam werden.

Speichern der UNIX-Einstellungen

Hinweis: Diese Vorgehensweise kann je nach UNIX®-Typ (z. B. Solaris™, IBM® AIX™) oder verwendeter Version leicht abweichen.

---

1. Wählen Sie "Style Manager" > "Startup" (Stilmanager > Start) aus. Das Dialogfeld "Startup" (Start) des Style Manager (Stilmanager) wird angezeigt.
2. Wählen Sie im Dialogfenster "Logout Confirmation" (Abmeldebestätigung) die Option "On" (Ein) aus. Bei dieser Option werden Sie dazu aufgefordert, Ihre aktuelle Sitzung zu speichern, wenn Sie sich abmelden.

Einstellungen für Apple Macintosh

Bei KVM-Zielservern, auf denen ein Apple Macintosh®-Betriebssystem ausgeführt wird, sollten Sie das D2CIM-VUSB und den Mausmodus "Absolute Mouse Synchronization" (Absolute Maussynchronisierung) verwenden.

Schritt 2: Konfigurieren der Einstellungen für die Netzwerkfirewall

Der Remotezugriff auf LX setzt voraus, dass das Netzwerk und die Firewall die Kommunikation über TCP-Port 5000 zulassen. LX kann auch zur Verwendung eines anderen TCP-Ports konfiguriert werden. In diesem Fall muss die Kommunikation über diesen Port zugelassen werden. Wenn Sie über einen Webbrowser auf LX zugreifen möchten, muss die Firewall darüber hinaus den Zugriff auf den TCP-Port 443 (Standard HTTPS) zulassen. Durch den Zugriff auf TCP-Port 80 (Standard HTTP) wird die automatische Umleitung von HTTP-Anfragen an HTTPS ermöglicht.



Schritt 3: Anschließen der Geräte



A. Wechselstromversorgung

▶ So schließen Sie die Stromversorgung an:

- Verbinden Sie das beiliegende Netzkabel mit LX, und schließen Sie es an die Wechselstromversorgung an.

B. Netzwerkports

▶ So stellen Sie eine Netzwerkverbindung her:

- Stellen Sie mit einem standardmäßigen Netzwerkkabel (im Lieferumfang enthalten) eine Verbindung zwischen dem Netzwerkport und einem Ethernet-Switch, -Hub oder -Router her.



C. Port für den lokalen Zugriff (lokaler PC)

Für den bequemen Zugriff auf Zielserver am Serverschrank kann der Port für den lokalen Zugriff von LX verwendet werden. Der Port für den lokalen Zugriff wird für die Installation und Konfiguration benötigt, die weitere Verwendung dieses Ports ist jedoch optional. Der Port für den lokalen Zugriff bietet eine grafische Benutzeroberfläche der lokalen LX-Konsole, die für die Verwaltung und für den Zugriff auf Zielserver verwendet wird. Weitere Informationen finden Sie unter Lokale Porteinstellungen für LX konfigurieren.

▶ So stellen Sie eine Verbindung zum lokalen Port her:

- Schließen Sie einen MultiSync-VGA-Monitor, eine Maus und eine Tastatur an die Ports mit der Bezeichnung "Local User" (lokaler Benutzer) an. Verwenden Sie eine USB-Tastatur und -Maus. Die Portanschlüsse befinden sich auf der Rückseite von LX.

Verbindung	Beschreibung
Monitor	Schließen Sie einen standardmäßigen MultiSync-VGA-Monitor am HD15-Videoport (weiblich) an.
Tastatur	Schließen Sie eine standardmäßige USB-Tastatur an einen der USB Typ A-Ports (weiblich) an.
Maus	Schließen Sie eine standardmäßige USB-Maus an einen der USB Typ A-Ports (weiblich) an.

D. Zielserverports

Für den bequemen Zugriff auf Zielserver am Serverschrank kann der Port für den lokalen Zugriff von LX verwendet werden. Der Port für den lokalen Zugriff wird für die Installation und Konfiguration benötigt, die weitere Verwendung dieses Ports ist jedoch optional. Der Port für den lokalen Zugriff bietet eine grafische Benutzeroberfläche der lokalen LX-Konsole, die für die Verwaltung und für den Zugriff auf Zielserver verwendet wird. Weitere Informationen finden Sie unter Lokale Porteinstellungen für LX konfigurieren.

▶ So stellen Sie eine Verbindung zwischen einem Zielserver und LX her:

1. Verwenden Sie das entsprechende CIM (Computer Interface Module). Weitere Informationen zu kompatiblen CIMs finden Sie unter ***Unterstützte Betriebssysteme (Clients)*** (auf Seite 228).

2. Schließen Sie das UTP-Kabel (Cat5/5e/6) Ihres CIM an den Videoport des Zielservers an. Stellen Sie sicher, dass die Grafikeinstellungen Ihres Zielservers bereits so konfiguriert sind, dass eine unterstützte Auflösung und Aktualisierungsfrequenz eingestellt sind. Stellen Sie bei Servern von Sun sicher, dass die Grafikkarte Ihres Zielservers so eingestellt ist, dass Standard-VGA (H- und V-Synchronisierung) und nicht Composite-Synchronisierung ausgegeben wird.
3. Schließen Sie den Tastatur-/Mausstecker des CIM an die entsprechenden Ports des Zielservers an. Verwenden Sie ein standardmäßiges Straight-Through-UTP-Kabel (Kat. 5/5e/6), um das CIM mit einem verfügbaren Serverport auf der Rückseite Ihres LX-Geräts zu verbinden.

Hinweis: D2CIM-USB G2 verfügt über einen kleinen Schiebeschalter auf der Rückseite des CIM. Schalten Sie den Schalter in Position "B" für PC-basierte USB-Zielserver. Schalten Sie den Schalter in Position "S" für Sun-USB-Zielserver.

Eine neue Switch-Position wird erst wirksam, wenn das CIM aus- und wieder eingeschaltet wird. Um das CIM aus- und wieder einzuschalten, entfernen Sie den USB-Stecker vom Zielserver und schließen Sie ihn nach einigen Sekunden erneut an.

E. Modemport (Optional)

LX besitzt einen dedizierten Modemport für den Remotezugriff, auch wenn das LAN/WAN nicht verfügbar ist. Verbinden Sie mithilfe eines seriellen (RS-232) Straight-Through-Kabels ein externes serielles Modem mit dem Port mit der Bezeichnung MODEM auf der Rückseite des LX. Eine Liste der zertifizierten Modems finden Sie unter ***Technische Daten*** (auf Seite 217) und Informationen zum Konfigurieren des Modems unter ***Konfigurieren der Modemeinstellungen*** (auf Seite 147).

Hinweis: Raritan empfiehlt, das Modem durch Aktivieren der Einstellung CD (Carrier Detect) zu konfigurieren.



Schritt 4: Konfigurieren von LX

Wenn Sie das LX-Gerät zum ersten Mal starten, müssen Sie einige Konfigurationseinstellungen über die lokale LX-Konsole vornehmen:

- Ändern des Standardkennworts
- Zuweisen der IP-Adresse
- Benennen der KVM-Zielserver

Sie können LX über einen Webbrowser konfigurieren. Hierzu muss auf Ihrer Workstation jedoch die entsprechende Version der Java Runtime Environment (JRE) installiert sein.

Ändern des Standardkennworts

LX wird mit einem Standardkennwort geliefert. Beim ersten Starten des LX müssen Sie dieses Kennwort ändern.

▶ So ändern Sie das Standardkennwort:

1. Geben Sie nach dem Bootvorgang der Einheit den Standardbenutzernamen (admin) und das Standardkennwort (raritan) ein. Klicken Sie auf "Login" (Anmelden).
2. Geben Sie das alte Kennwort (raritan), ein neues Kennwort und anschließend erneut das neue Kennwort ein. Ein Kennwort kann aus bis zu 64 alphanumerischen Zeichen der englischen Sprache sowie Sonderzeichen bestehen. Klicken Sie auf "Apply" (Übernehmen). Klicken Sie auf der Seite "Confirmation" (Bestätigung) auf "OK".

Hinweis: Das Standardkennwort kann auch mittels des Multi-Platform-Clients (MPC) von Raritan geändert werden.

Zuweisen einer IP-Adresse

Im Folgenden wird das Zuweisen einer IP-Adresse auf der Seite "Network Settings" (Netzwerkeinstellungen) beschrieben. Umfassende Informationen zu allen Feldern sowie zur Funktionsweise dieser Seite finden Sie unter ***Netzwerkeinstellungen*** (siehe "***Network Settings (Netzwerkeinstellungen)***" auf Seite 134).

▶ So weisen Sie eine IP-Adresse zu:

1. Wählen Sie "Device Settings > Network" (Geräteeinstellungen > Netzwerk). Die Seite "Network Settings" (Netzwerkeinstellungen) wird angezeigt.
2. Geben Sie einen aussagekräftigen Namen für Ihr LX-Gerät an. Verwenden Sie dazu bis zu 32 gültige Sonderzeichen und keine Leerzeichen.



3. Geben Sie im Bereich "IPv4" die entsprechenden IPv4-spezifischen Netzwerkeinstellungen ein oder wählen Sie diese aus:

   a. Geben Sie eine IP-Adresse ein, falls erforderlich. Die Standard-IP-Adresse lautet 192.168.0.192.

   b. Geben Sie die Subnetzmaske ein. Die Standardsubnetzmaske lautet 255.255.255.0.

   c. Geben Sie das Standardgateway ein, wenn in der Dropdownliste unter "IP Auto Configuration" (Automatische IP-Konfiguration) "None" (Keine) ausgewählt ist.

   d. Geben Sie den Namen des bevorzugten DHCP-Hosts ein, wenn in der Dropdownliste unter "IP Auto Configuration" (Automatische IP-Konfiguration) "DHCP" ausgewählt ist.

   e. Wählen Sie "IP Auto Configuration" (Automatische IP-Konfiguration) aus. Folgende Optionen stehen zur Verfügung:

   - None (Static IP) [Keine (Statisches IP)] – Bei Auswahl dieser Option müssen Sie die Netzwerkparameter manuell angeben.

     Diese Option wird empfohlen, da LX ein Infrastrukturgerät ist, dessen IP-Adresse sich nicht ändern sollte.

   - DHCP – Dynamic Host Configuration Protocol wird von Netzwerkcomputern (Clients) verwendet, um eindeutige IP-Adressen und andere Parameter von einem DHCP-Server zu erhalten.

     Bei Auswahl dieser Option werden die Netzwerkparameter vom DHCP-Server zugewiesen. Bei Verwendung von DHCP geben Sie unter "Preferred host name (DHCP only)" (Name des bevorzugten Hosts [Nur DHCP]) einen Wert ein (maximal 63 Zeichen).

4. Wenn IPv6 verwendet werden soll, geben Sie im Bereich "IPv6" die entsprechenden IPv6-spezifischen Netzwerkeinstellungen ein oder wählen Sie diese aus:

   a. Aktivieren Sie das Kontrollkästchen "IPv6", um die Felder in diesem Bereich zu aktivieren.

   b. Geben Sie eine globale/eindeutige IP-Adresse ein. Dies ist die IP-Adresse, die dem LX zugeordnet ist.

   c. Geben Sie die Präfixlänge ein. Dies ist die Anzahl der Bits, die in der IPv6-Adresse verwendet werden.

   d. Geben Sie die IP-Adresse des Gateway ein.

   e. Link-Local-IP-Adresse. Diese Adresse wird dem Gerät automatisch zugewiesen. Sie wird zum Erkennen von Nachbarn verwendet oder wenn keine Router verfügbar sind. **Read-Only (Lese-zugriff)**



f. Zonen-ID. Hierdurch wird das Gerät identifiziert, dem die Adresse zugeordnet ist. **Read-Only (Lese-zugriff)**

g. Wählen Sie "IP Auto Configuration" (Automatische IP-Konfiguration) aus. Folgende Optionen stehen zur Verfügung:

- None (Keine) – Wählen Sie diese Option aus, wenn Sie keine automatische IP-Konfiguration wünschen, sondern die IP-Adresse lieber selbst festlegen (statisches IP). Diese Option ist voreingestellt und wird empfohlen.

  Wenn für "IP auto configuration" (Automatische IP-Konfiguration) "None" (Keine) ausgewählt ist, sind die folgenden "Network Basic Settings" (Basisnetzwerkeinstellungen) aktiviert: "Global/Unique IP Address" (Globale/Eindeutige IP-Adresse), "Prefix Length" (Präfixlange) und "Gateway IP Address" (Gateway-IP-Adresse) ermöglichen Ihnen die manuelle IP-Konfiguration.

- Router Discovery (Router-Erkennung) – Verwenden Sie diese Option, um IPv6-Adressen, deren Signifikanz "Global" oder "Unique Local" (Lokal eindeutig) ist und über der von Link Local liegt, welche nur für ein direkt verbundenes Subnetz gültig ist, automatisch zuzuordnen.

5. Wenn DHCP ausgewählt ist, wählen Sie "Obtain DNS Server Address Automatically" (DNS-Serveradresse automatisch abrufen) aus, um diese Funktion zu aktivieren. Wenn die DNS-Serveradresse automatisch abgerufen wird, werden die vom DHCP-Server bereitgestellten DNS-Informationen verwendet.

6. Wenn "Use the Following DNS Server Addresses" (Die folgenden DNS-Serveradressen verwenden) ausgewählt ist, werden die in diesem Abschnitt eingegebenen Adressen für die Verbindung zum DNS-Server verwendet, unabhängig davon, ob DHCP ausgewählt wurde.

   Geben Sie die folgenden Informationen ein, wenn die Option "Following DNS Server Addresses" (Folgende DNS-Serveradressen) ausgewählt wurde. Diese Adressen sind die primären und sekundären DNS-Adressen, die verwendet werden, wenn die primäre DNS-Serververbindung aufgrund eines Ausfalls getrennt wird.

   a. Primary DNS Server IP Address (IP-Adresse des primären DNS-Servers)

   b. Secondary DNS-Server IP Address (IP-Adresse des sekundären DNS-Servers)

7. Klicken Sie abschließend auf OK.



Weitere Informationen zur Konfiguration dieses Bereichs der Seite "Network Settings" (Netzwerkeinstellungen) finden Sie unter LAN-Schnittstelleneinstellungen.

Hinweis: Bei manchen Umgebungen gibt die Standardeinstellung "Autodetect" (automatische Aushandlung) für "LAN Interface Speed & Duplex" (LAN-Schnittstellengeschwindigkeit und Duplex) die Netzwerkparameter nicht richtig vor, was zu Netzwerkproblemen führen kann. Wählen Sie in einem solchen Fall im Feld "LAN Interface Speed & Duplex" des LX den Wert "100 Mbps/Full Duplex" (100 Mbit/s/Vollduplex) (bzw. die geeignete Option für Ihr Netzwerk) aus, um dieses Problem zu beheben.Weitere Informationen finden Sie auf der Seite **Network Settings** *(siehe "***Network Settings (Netzwerkeinstellungen)***" auf Seite 134)* *(Netzwerkeinstellungen).*

Konfigurieren von Datum-/Uhrzeiteinstellungen (optional)

▶ **So stellen Sie das Datum und die Uhrzeit ein:**

1. Wählen Sie "Device Settings > Date/Time"(Geräteeinstellungen > Datum/Uhrzeit). Die Seite "Date/Time Settings" (Datum-/Uhrzeiteinstellungen) wird angezeigt.
2. Wählen Sie in der Dropdown-Liste "Time Zone" Ihre Zeitzone aus.
3. Aktivieren Sie das Kontrollkästchen "Adjust for daylight savings time" (an Sommerzeit anpassen), um die Uhrzeit an die Sommerzeit anzupassen.
4. Wählen Sie eine Methode, um Datum und Uhrzeit einzustellen:
   - "User Specified Time" (Benutzerdefinierte Zeit) – Bei dieser Option können Sie Datum und Uhrzeit manuell eingeben. Falls Sie die Option "User Specified Time" (Benutzerdefinierte Zeit) ausgewählt haben, geben Sie Datum und Uhrzeit wie folgt ein: Geben Sie im Feld "Time" die Uhrzeit im Format hh:mm ein. (Verwenden Sie das 24-h-Zeitformat.)
   - "Synchronize with NTP Server" (Mit NTP-Server synchronisieren) – Bei dieser Option können Sie Datum und Uhrzeit mit dem NTP (Network Time Protocol)-Server synchronisieren.
5. Falls Sie die Option "Synchronize with NTP Server" (Mit NTP-Server synchronisieren) ausgewählt haben, gehen Sie folgendermaßen vor:
   a. Geben Sie im Feld "Primary Time Server" (Primärer Zeitserver) die IP-Adresse dieses Servers ein.
   b. Geben Sie im Feld "Secondary Time Server" (Sekundärer Zeitserver) die IP-Adresse dieses Servers ein. ***///Optional***
6. Klicken Sie auf "OK".



Benennen der Zielserver

So benennen Sie die Zielserver:

1. Schließen Sie alle Zielserver an, falls dies noch nicht geschehen ist. Weitere Einzelheiten finden Sie unter **Schritt 3: Anschließen der Geräte** für eine Beschreibung zum Anschließen der Geräte.
2. Wählen Sie mithilfe der lokalen LX-Konsole "Device Settings > Port Configuration" (Geräteeinstellungen > Portkonfiguration) und klicken Sie anschließend auf den Portnamen des Zielservers, den Sie benennen möchten.
3. Geben Sie einen Namen für den Server ein, der maximal 32 alphanumerische Zeichen und Sonderzeichen umfasst. Klicken Sie auf "OK".

Gültige Sonderzeichen für Zielnamen

Zeichen	Beschreibung	Zeichen	Beschreibung
!	Ausrufezeichen	;	Strichpunkt
"	Doppeltes Anführungszeichen	=	Gleichheitszeichen
#	Raute	>	Größer-als-Zeichen
$	Dollarzeichen	?	Fragezeichen
%	Prozentzeichen	@	At-Zeichen
&	Kaufmännisches Und	[	Linke eckige Klammer
(	Linke runde Klammer	\	Umgekehrter Schrägstrich
)	Rechte runde Klammer	]	Rechte eckige Klammer
*	Sternchen	^	Zirkumflexzeichen
+	Pluszeichen	_	Unterstreichungszeichen
,	Komma	`	Graviszeichen
-	Bindestrich	{	Linke geschweifte Klammer
.	Punkt	|	Senkrechter Strich
/	Schrägstrich	}	Rechte geschweifte



Zeichen	Beschreibung	Zeichen	Beschreibung
			Klammer
<	Kleiner-als-Zeichen	~	Tilde
:	Doppelpunkt		

Remoteauthentifizierung

Unterstützte Protokolle

Zur Vereinfachung der Verwaltung von Benutzernamen und Kennwörtern bietet LX die Möglichkeit, Authentifizierungsanforderungen an einen externen Authentifizierungsserver weiterzuleiten. Zwei externe Authentifizierungsprotokolle werden unterstützt: LDAP/LDAPS und RADIUS.

Hinweis zu Microsoft Active Directory

Microsoft® Active Directory® verwendet nativ das LDAP/LDAPS-Protokoll und kann als LDAP/LDAPS-Server und Authentifizierungsquelle für LX fungieren. Bei Verwendung der IAS-Komponente (Internetautorisierungsserver) kann ein Microsoft Active Directory-Server auch als RADIUS-Authentifizierungsquelle dienen.

Erstellen von Benutzergruppen und Benutzern

Im Rahmen der Erstkonfiguration müssen Sie Benutzergruppen und Benutzer definieren, damit Benutzer auf LX zugreifen können.

LX verwendet im System bereits vorhandene Standardbenutzergruppen und ermöglicht es Ihnen, Gruppen zu erstellen und entsprechende Berechtigungen für sie festzulegen.

Für den Zugriff auf LX sind ein Benutzername und ein Kennwort erforderlich. Anhand dieser Informationen werden Benutzer authentifiziert, die versuchen, auf LX zuzugreifen. Weitere Informationen zum Hinzufügen oder Bearbeiten von Benutzergruppen und Benutzern finden Sie unter **Benutzerverwaltung** (siehe "**User Management (Benutzerverwaltung)**" auf Seite 110).

Schritt 5: Starten der LX-Remotekonsole

So starten Sie die LX-Remote-Konsole:

1. Melden Sie sich bei einer Workstation an, die eine Netzwerkverbindung zum LX herstellen kann und auf der Microsoft .NET® bzw. Java Runtime Environment® installiert ist (JRE® ist auf der ***Java-Website http://java.sun.com/*** verfügbar).



2. Starten Sie einen unterstützten Webbrowser, z. B. Internet Explorer® oder Firefox®.
3. Geben Sie die URL ein: *http://IP-ADRESSE* bzw. *http://IP-ADRESSE/akc* für .NET, wobei IP-ADRESSE die dem LX zugewiesene IP-Adresse ist. Sie können auch "https" verwenden, den vom Administrator zugewiesenen DNS-Namen des LX (sofern ein DNS-Server konfiguriert wurde), oder die IP-Adresse im Browser eingeben (LX leitet die IP-Adresse stets von HTTP zu HTTPS um).
4. Geben Sie Ihren Benutzernamen und das Kennwort ein. Klicken Sie auf "Login" (Anmelden).

Remotezugriff und Remotesteuerung der Zielserver

Auf der LX-Seite "Port Access" (Portzugriff) werden die LX-Ports und die verbundenen Zielserver sowie Angaben zu Status und Verfügbarkeit der Ports angezeigt.

Zugreifen auf einen Zielserver

► **So greifen Sie auf einen Zielserver zu:**

1. Klicken Sie auf den Portnamen des Zielgeräts, auf das Sie zugreifen möchten. Das Menü "Port Action" (Portaktion) wird angezeigt.
2. Wählen Sie im Menü "Port Action" (Portaktion) die Option "Connect" (Verbinden) aus. Ein KVM-Fenster wird geöffnet, das eine Verbindung zum Ziel anzeigt.

Wechseln zwischen Zielservern

► **So wechseln Sie zwischen KVM-Zielservern:**

1. Rufen Sie die LX-Seite "Port Access" (Portzugriff) auf, während bereits auf einen Zielserver zugegriffen wird.
2. Klicken Sie auf den Portnamen des Zielgeräts, auf das Sie zugreifen möchten. Das Menü "Port Action" (Portaktion) wird angezeigt.
3. Wählen Sie im Menü "Port Action" (Portaktion) die Option "Switch From" (Wechseln von) aus. Der neue Zielserver, den Sie ausgewählt haben, wird angezeigt.

Trennen eines Zielservers

► **So trennen Sie einen Zielserver:**

- Klicken Sie auf den Portnamen des Zielgeräts, das Sie trennen möchten. Wenn das Menü "Port Action" (Portaktion) angezeigt wird, klicken Sie auf "Disconnect" (Trennen).

Schritt 6: Konfigurieren der Tastatursprache (optional)

Hinweis: Dieser Schritt ist nicht erforderlich, wenn Sie eine US-/internationale Tastatur verwenden.

Wenn Sie eine andere Tastatur verwenden, muss diese für die jeweilige Sprache konfiguriert werden. Außerdem muss die Tastatursprache für das Client-Gerät mit der der KVM-Zielserver übereinstimmen.

Weitere Informationen zum Ändern des Tastaturlayouts finden Sie in der Dokumentation Ihres Betriebssystems.

Ändern des Tastatur-Layout-Codes (Sun-Zielgeräte)

Gehen Sie folgendermaßen vor, wenn Sie ein DCIM-SUSB verwenden und das Tastaturlayout auf eine andere Sprache ändern möchten.

- **So ändern Sie den Tastaturlayoutcode (nur DCIM-SUSB):**

1. Öffnen Sie auf der Sun™-Workstation ein Texteditorfenster.
2. Vergewissern Sie sich, dass die Taste "Num Lock" aktiviert ist, und drücken Sie die linke Strg-Taste und die Taste "Entf" auf der Tastatur. Die LED der Feststelltaste beginnt zu blinken, was darauf hindeutet, dass sich das CIM im Modus zum Ändern des Layoutcodes befindet. Im Textfenster wird Folgendes angezeigt: `Raritan Computer, Inc. Current keyboard layout code = 22h (US5 UNIX)` [Raritan Computer, Inc. Aktueller Tastaturlayoutcode = 22h (US5 UNIX)].
3. Geben Sie den gewünschten Layoutcode ein (für eine japanische Tastatur beispielsweise *31*).
4. Drücken Sie die Eingabetaste.
5. Schalten Sie das Gerät aus und wieder ein. Das DCIM-SUSB wird zurückgesetzt (Aus- und Einschalten).
6. Überprüfen Sie, ob die Zeichen korrekt sind.



Schritt 7: Konfigurieren von Schichten (optional)

LX und generische Schichten werden von LX unterstützt. Weitere Informationen zu dieser Funktion finden Sie im Abschnitt **Geräteverwaltung** (auf Seite 134).

Verbinden Sie einen Zielserverport auf dem Basisgerät mithilfe eines D2CIM-DVUSB mit dem lokalen Port des LX-Schichtgeräts (Video-/Tastatur-/Mausports).

▶ So aktivieren Sie Schichten:

1. Wählen Sie von der Schichtbasis "Device Settings" > "Device Services" (Geräteeinstellungen > Gerätedienste) aus. Die Seite "Device Service Settings" (Gerätediensteinstellungen) wird angezeigt.
2. Wählen Sie "Enable Tiering as Base" (Schichten als Basis aktivieren) aus.
3. Geben Sie in das Feld "Base Secret" (Geheimer Basisschlüssel) den geheimen Schlüssel ein, der von den Basis- und Schichtgeräten gemeinsam verwendet wird. Dieser geheime Schlüssel ist für die Schichtgeräte zur Authentifizierung des Basisgeräts erforderlich. Sie müssen denselben geheimen Schlüssel für das Schichtgerät eingeben.
4. Klicken Sie auf OK.
5. Aktivieren Sie die Schichtgeräte. Wählen Sie auf dem Schichtgerät "Device Settings" > "Local Port Settings" (Geräteeinstellungen > Lokale Porteinstellungen) aus.
6. Wählen Sie im Bereich "Enable Local Ports" (Lokale Ports aktivieren) die Option "Enable Local Port Device Tiering" (Lokaler Port für Geräteschichten aktivieren) aus.
7. Geben Sie im Feld "Tier Secret" (Geheimer Schlüssel der Schicht) denselben geheimen Schlüssel ein, den Sie für das Basisgerät auf der Seite "Device Settings" (Geräteeinstellungen) eingegeben haben.
8. Klicken Sie auf OK.

Kapitel 3 Arbeiten mit Zielservern

In diesem Kapitel

LX-Schnittstellen

LX bietet Ihnen verschiedene Benutzeroberflächen, über die Sie jederzeit und überall einfach auf die Ziele zugreifen können. Dazu zählen die lokale LX-Konsole, die LX-Remotekonsole, der Virtual KVM Client (VKC), der Active KVM Client (AKC) und der Multi-Platform-Client (MPC). In der folgenden Tabelle werden diese Oberflächen und ihre Nutzung für den Zielserverzugriff und die lokale sowie die Remoteverwaltung erläutert:

Benutzeroberfläche	Lokal		Remote	
	Access (Zugriff)	**Admin**	**Access (Zugriff)**	**Admin**
Lokale LX-Konsole	✓	✓		
LX-Remotekonsole			✓	✓
Virtual KVM Client (VKC)			✓	
Multi-Platform-Client (MPC)			✓	✓
Active KVM Client (AKC)			✓	✓

Die folgenden Abschnitte des Hilfedokuments enthalten Informationen zur Verwendung spezieller Oberflächen, um auf LX zuzugreifen und Zielgeräte zu verwalten.

- Lokale Konsole
- Remotekonsole
- Virtual KVM Client
- Multi-Platform-Client

Oberfläche der lokalen LX-Konsole: LX-Geräte

Am Serverschrank erfüllt LX über die lokale LX-Konsole standardmäßige KVM-Management- und Verwaltungsfunktionen. Die lokale LX-Konsole stellt eine direkte KVM-Verbindung (analog) mit den angeschlossenen Servern her. Die Leistung ist mit der Leistung bei einer direkten Verbindung mit der Tastatur, der Maus und den Videoports des Servers identisch.

Die grafischen Benutzeroberflächen der lokalen LX-Konsole und der LX-Remotekonsole verfügen über zahlreiche Gemeinsamkeiten. Auf die Unterschiede wird in diesem Hilfedokument hingewiesen.

Die LX-Option "Local Console Factory Reset" (Werksrücksetzung der lokalen Konsole) ist bei der lokalen LX-Konsole verfügbar, jedoch nicht bei der LX-Remotekonsole.

Oberfläche der LX-Remotekonsole

Die LX-Remotekonsole ist eine browserbasierte grafische Benutzeroberfläche, mit der Sie sich an KVM-Zielservern und seriellen Zielgeräten, die mit LX verbunden sind, anmelden und LX von einem Remotestandort aus verwalten können.

Die LX-Remotekonsole bietet eine digitale Verbindung mit den angeschlossenen KVM-Zielservern. Wenn Sie sich über die LX-Remotekonsole bei einem KVM-Zielserver anmelden, wird ein Fenster für den Virtual KVM Client geöffnet.

Die grafischen Benutzeroberflächen der lokalen LX-Konsole und der LX-Remotekonsole verfügen über zahlreiche Gemeinsamkeiten. Auf die Unterschiede wird in diesem Benutzerhandbuch hingewiesen. Die folgenden Optionen stehen nur für die LX-Remotekonsole, nicht jedoch für die lokale LX-Konsole zur Verfügung:

- Virtuelle Medien
- Favorites (Favoriten)
- Backup/Restore (Sicherung/Wiederherstellung)
- Firmware Upgrade (Firmware-Aktualisierung)
- SSL-Zertifikate

Starten der LX-Remotekonsole

Wichtig: Unabhängig vom verwendeten Browser müssen Popups für die IP-Adresse des Geräts zugelassen werden, damit die LX-Remotekonsole gestartet werden kann.

Abhängig von den Browser- und Sicherheitseinstellungen werden möglicherweise verschiedene Sicherheits- und Zertifikatwarnungen angezeigt. Sie müssen diese Warnungen bestätigen, um die LX-Remotekonsole zu starten.

Sie können die Zahl der Warnmeldungen zur Sicherheit und zu Zertifikaten für zukünftige Anmeldungen reduzieren, indem Sie darin die folgenden Kontrollkästchen aktivieren:

- In the future, do not show this warning (Diese Warnung nicht mehr anzeigen).
- Always trust content from this publisher (Inhalt von diesem Herausgeber immer vertrauen).

So starten Sie die LX-Remote-Konsole:

1. Melden Sie sich bei einer Workstation an, die eine Netzwerkverbindung zum LX herstellen kann und auf der Microsoft .NET® bzw. Java Runtime Environment® installiert ist (JRE® ist auf der ***Java-Website http://java.sun.com/*** verfügbar).
2. Starten Sie einen unterstützten Webbrowser, z. B. Internet Explorer® oder Firefox®.
3. Geben Sie die URL ein: *http://IP-ADRESSE* bzw. *http://IP-ADRESSE/akc* für .NET, wobei IP-ADRESSE die dem LX zugewiesene IP-Adresse ist. Sie können auch "https" verwenden, den vom Administrator zugewiesenen DNS-Namen des LX (sofern ein DNS-Server konfiguriert wurde), oder die IP-Adresse im Browser eingeben (LX leitet die IP-Adresse stets von HTTP zu HTTPS um).
4. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein. Wenn Sie sich zum ersten Mal anmelden, geben Sie den/das werkseitig voreingestellte(n) Benutzernamen (admin) und Kennwort (raritan, beides kleingeschrieben) ein. Sie werden aufgefordert, das Standardkennwort zu ändern. Klicken Sie auf "Login" (Anmelden).

Weitere Informationen zu den LX-Funktionen, die über die Remotekonsole verfügbar sind, finden Sie unter ***Virtual KVM Client (VKC) und Active KVM Client (AKC)*** (auf Seite 60).



Oberfläche und Navigation

LX-Schnittstelle

Die LX-Remotekonsole und die lokale LX-Konsole bieten für die Konfiguration und Verwaltung des Geräts eine webbasierte Oberfläche sowie eine Liste und Auswahl der Zielserver. Die Optionen befinden sich auf verschiedenen Registerkarten.

Nachdem Sie sich erfolgreich angemeldet haben, wird die Seite "Port Access" (Portzugriff) angezeigt, in der alle Ports mit ihrem Status und ihrer Verfügbarkeit aufgeführt sind. Auf der Seite sind zwei Registerkarten verfügbar: "View by Port" (Ansicht nach Port) und "Set Scan" (Scanfunktion einstellen). Klicken Sie auf der Registerkarte "View by Port" (Ansicht nach Port) auf eine Spaltenüberschrift, um die Ports nach "Port Number" (Portnummer), "Port Name" (Portname), "Status (Up oder Down)" (Status (Ein oder Aus)) und "Availability (Idle, Connected, Busy, Unavailable und Connecting)" (Verfügbarkeit (Inaktiv, Verbunden, Verwendet, Nicht verfügbar und Verbindung wird hergestellt)) zu sortieren. Ändern Sie die Anzahl der Ports, die auf der Seite angezeigt werden, indem Sie in das Feld "Rows per Page" (Zeilen pro Seite) unten rechts auf der Seite eine Zahl eingeben und dann auf "Set" (Festlegen) klicken. Weitere Informationen finden Sie unter ***Seite "Port Access" (Portzugriff)*** (siehe "***Seite "Port Access" (Port-Zugriff)***" auf Seite 48).

Auf der Registerkarte "Set Scan" (Scanfunktion einstellen) können Sie außerdem nach bis zu 32 Zielen suchen, die mit dem LX verbunden sind. Siehe ***Scannen von Ports*** (auf Seite 51).



Linker Bildschirmbereich

Der linke Bildschirmbereich der LX-Oberfläche enthält folgende Informationen. Beachten Sie, dass die Anzeige einiger Informationen abhängig vom Benutzer, von der verwendeten Funktion usw. ist. Die bedingten Informationen werden nachfolgend aufgeführt.

Informationen	Beschreibung	Anzeige
Zeit & Sitzung	Datum und Uhrzeit, wann die aktuelle Sitzung begonnen hat.	Immer
Benutzer	Benutzername	Immer
Status	Der aktuelle Status der Anwendung, entweder inaktiv oder aktiv. Bei Inaktivität zeichnet die Anwendung die Uhrzeit der inaktiven Sitzung auf und zeigt diese an.	Immer
Ihre IP	Die für den Zugriff auf LX verwendete IP-Adresse.	Immer
Letzte Anmeldung	Datum und Uhrzeit der letzten Anmeldung.	Immer
Device Information (Geräteinformation en)	Informationen zum verwendeten LX.	Immer
Gerätename	Dem Gerät zugewiesener Name.	Immer
IP-Adresse	Die IP-Adresse des LX.	Immer
Firmware	Aktuelle Version der Firmware.	Immer
Gerätemodell	Modell des LX	Immer
Als Basis oder als Schicht konfiguriert*	Wenn Sie eine Schichtkonfiguration verwenden, wird hier angezeigt, ob es sich bei LX, auf das Sie zugreifen, um das Basis- oder Schichtgerät handelt.	Wenn LX Teil einer Schichtkonfiguration ist.



Informationen	Beschreibung	Anzeige
Portstatus	Die Status der Ports, die von LX verwendet werden.	Immer
Verbundene Benutzer	Die Benutzer, identifiziert durch Benutzername und IP-Adresse, die aktuell mit LX verbunden sind.	Immer
Online-Hilfe	Verknüpfung zur Online-Hilfe.	Immer
Bevorzugte Geräte	Siehe ***Verwalten von Favoriten*** (auf Seite 54).	Immer

Navigation in der LX-Konsole

In den Oberflächen der LX-Konsolen haben Sie viele Möglichkeiten für die Navigation und Auswahl.

- **Für die Auswahl von Optionen stehen folgende Möglichkeiten zur Verfügung:**

- Klicken Sie auf eine Registerkarte. Eine Seite mit verfügbaren Optionen wird angezeigt.
- Zeigen Sie mit dem Cursor auf eine Registerkarte und wählen Sie die gewünschte Option aus dem Menü aus.
- Klicken Sie in der angezeigten Menühierarchie (den sogenannten "Breadcrumbs") direkt auf die gewünschte Option.

- **So blättern Sie durch Seiten, die größer als der Bildschirm sind:**

- Verwenden Sie die Bild-Auf- und Bild-Ab-Tasten der Tastatur.
- Verwenden Sie die Bildlaufleiste auf der rechten Seite.

Seite "Port Access" (Port-Zugriff)

Nachdem Sie sich erfolgreich bei der LX-Remotekonsole angemeldet haben, wird die Seite "Port Access" (Portzugriff) angezeigt. Standardmäßig wird die Registerkarte "View by Port" (Ansicht nach Port) auf der Seite "Port Access" (Portzugriff) angezeigt. Diese Seite enthält alle LX-Ports, die angeschlossenen KVM-Zielserver sowie deren Status und Verfügbarkeit. Über die Seite "Port Access" (Portzugriff) haben Sie Zugriff auf die mit LX verbundenen KVM-Zielserver. KVM-Zielserver sind Server, die Sie über das LX-Gerät steuern möchten. Sie sind mit den LX-Ports auf der Rückseite des Geräts verbunden.

Hinweis: Für jede Verbindung mit einem KVM-Zielserver wird ein neues Fenster für den Virtual KVM Client geöffnet.

Wenn Sie eine Schichtkonfiguration verwenden, in der ein LX-Basisgerät für den Zugriff auf mehrere andere Schichtgeräte verwendet wird, werden die Schichtgeräte auf der Seite "Port Access" (Portzugriff) angezeigt, wenn Sie auf das Symbol "Expand Arrow" (Pfeil erweitern) ▶ links neben dem Schichtgerätenamen klicken. Weitere Informationen zu Schichten finden Sie unter ***Konfigurieren und Aktivieren von Schichten*** (auf Seite 142).

Über die Registerkarte "Set scan" (Scanfunktion einstellen) auf der Seite "Port Access" (Portzugriff) greifen Sie auf die Port-Scanfunktion zu. Mit dieser Funktion können Sie eine Reihe von zu scannenden Zielen festlegen. Die gescannten Ziele sind als Miniaturansicht verfügbar. Wählen Sie eine Miniaturansicht aus, um das entsprechende Ziel im Fenster des Virtual KVM Client zu öffnen.

▶ So verwenden Sie die Seite "Port Access" (Portzugriff):

1. Klicken Sie in der LX-Remotekonsole auf die Registerkarte "Port Access" (Portzugriff). Die Seite "Port Access" (Portzugriff) wird angezeigt.

   Die KVM-Zielserver werden zuerst nach Portnummer sortiert. Sie können die Anzeige so ändern, dass nach einer beliebigen Spalte sortiert wird.

   - Port Number (Portnummer) – Die für das LX-Gerät verfügbaren Ports werden beginnend mit 1 durchnummeriert.
   - Port Name (Portname) – Der Name des LX-Ports. Standardmäßig lautet dieser "Dominion-LX-Port#", Sie können den Namen jedoch durch einen aussagekräftigeren ersetzen. Wenn Sie auf einen Portnamenlink klicken, wird das Menü "Port Action" (Portaktion) geöffnet.

   Hinweis: Verwenden Sie für den Port (CIM)-Namen keine Auslassungszeichen (Apostroph).



- "Type" (Typ) – Der Server- oder CIM-Typ.
- "Status" (Status) – Der Status für Standardserver lautet entweder "Up" (Ein) oder "Down" (Aus).
- "Availability" (Verfügbarkeit) – Die Verfügbarkeit des Servers.

2. Klicken Sie auf den Portnamen des Zielservers, auf den Sie zugreifen möchten. Das Menü "Port Action" (Portaktion) wird angezeigt. Informationen zu verfügbaren Menüoptionen finden Sie unter Menü "Port Action" (Portaktion).
3. Wählen Sie im Menü "Port Action" (Portaktion) den gewünschten Menübefehl aus.
4. Legen Sie einen Satz von Ports fest, die auf dem LX mit der Funktion "Set Scan" (Scanfunktion einstellen) gescannt werden sollen. Siehe ***Scannen von Ports*** (auf Seite 51).

So ändern Sie die Sortierreihenfolge der Anzeige und/oder zeigen mehr Ports auf einer Seite an:

1. Klicken Sie auf die Spaltenüberschrift, nach der sortiert werden soll. Die Liste der KVM-Zielserver wird nach dieser Spalte sortiert.
2. Geben Sie im Abschnitt "Rows per Page" (Zeilen pro Seite) die Anzahl der Ports ein, die auf der Seite angezeigt werden sollen, und klicken Sie dann auf "Set" (Festlegen).

Menü "Port Action" (Portaktion)

Wenn Sie in der Liste "Port Access" (Portzugriff) auf einen Portnamen klicken, wird das Menü "Port Action" (Portaktion) angezeigt. Wählen Sie die gewünschte Menüoption für den Port aus. Beachten Sie, dass nur je nach Status und Verfügbarkeit des Ports aktuell verfügbare Optionen im Menü "Port Action" (Portaktion) aufgelistet werden:

- Connect (Verbinden) – Erstellt eine neue Verbindung mit dem Zielserver. Für die LX-Remotekonsole wird eine neue Virtual KVM Client-Seite angezeigt. Für die lokale LX-Konsole wechselt die Anzeige von der lokalen Benutzeroberfläche hin zum Zielserver. Auf dem lokalen Port muss die Oberfläche der lokalen LX-Konsole angezeigt werden, um den Wechsel durchführen zu können. Das Wechseln über Zugriffstasten ist vom lokalen Port auch verfügbar.

Hinweis: Diese Option steht in der LX-Remotekonsole für einen verfügbaren Port nicht zur Verfügung, wenn alle Verbindungen verwendet werden.

- Switch From (Wechseln von) – Wechselt von einer bestehenden Verbindung zum gewählten Port (KVM-Zielserver). Diese Menüoption ist nur für KVM-Zielgeräte verfügbar. Diese Option wird nur angezeigt, wenn der Virtual KVM Client geöffnet ist.

Hinweis: Diese Menüoption steht auf der lokalen LX-Konsole nicht zur Verfügung.

- Disconnect (Trennen) – Trennt diese Portverbindung und schließt die Seite des Virtual KVM Client für diesen Zielserver. Diese Menüoption ist nur für den Portstatus Up (Ein) und die Verfügbarkeit Connected (Verbunden) bzw. Up (Ein) und Busy (Verwendet) verfügbar.

Hinweis: Diese Menüoption steht auf der lokalen LX-Konsole nicht zur Verfügung. Sie können die Verbindung zum gewechselten Zielgerät auf der lokalen Konsole nur trennen, indem Sie die Zugriffstaste verwenden.



Scannen von Ports

LX ermöglicht eine Port-Scanfunktion, mit der nach ausgewählten Zielen gesucht werden kann. Die Ziele werden dann in einer Bildschirmpräsentationsansicht angezeigt. So können Sie bis zu 32 Ziele gleichzeitig überwachen. Sie können je nach Bedarf eine Verbindung mit mehreren Zielen herstellen oder sich auf ein bestimmtes Ziel konzentrieren. Scanvorgänge können Standardserver, Dominion-Schichtgeräte und KVM-Switch-Ports umfassen.

Hinweis: Scanvorgänge für Schichtgeräte werden vom Multi-Platform-Client (MPC) nicht unterstützt.

Beim Starten eines Scanvorgangs wird das Fenster "Port Scan" (Port-Scan) geöffnet. Jedes gefundene Ziel wird als Miniaturansicht in einer Bildschirmpräsentation angezeigt. In der Bildschirmpräsentation wird in einem Standardintervall von 10 Sekunden oder in dem von Ihnen angegebenen Intervall durch die Miniaturansichten der Ziele geblättert. Beim Blättern durch die Ziele wird das Ziel, das sich im Fokus der Bildschirmpräsentation befindet, in der Mitte der Seite angezeigt. Siehe ***Scaneinstellungen*** (siehe "***"Scan Settings" (Scaneinstellungen)***" auf Seite 90).

Die Zeit, mit der die Miniaturansichten in der Bildschirmpräsentation wechseln, den Fokusintervall der Miniaturansichten und die Anzeigeeinstellungen der Seite können Sie auf der Registerkarte "Scan Settings" (Scaneinstellungen) im Dialogfeld "Tools" (Extras) > "Options" (Optionen) des Virtual KVM Client (VKC), des Active KVM Client (AKC) und des Multi-Platform-Client (MPC) ändern. Siehe ***Scaneinstellungen*** (siehe "***"Scan Settings" (Scaneinstellungen)***" auf Seite 90).

Der Name des Ziels wird unter der entsprechenden Miniaturansicht und in der Taskleiste unten im Fenster angezeigt. Ist ein Ziel belegt, wird statt der Seite zum Zugreifen auf den Zielserver ein leerer Bildschirm angezeigt.

Der Status der einzelnen Ziele wird durch grüne, gelbe und rote Anzeigen angegeben, die unter der Zielminiaturansicht sowie in der Taskleiste angezeigt werden, wenn sich der Zielserver im Fokus der Bildschirmpräsentation befindet. Die Statusanzeigen geben Folgendes an:

- Grün – Das Ziel ist "up/idle" (ein/inaktiv) oder "up/connected" (ein/verbunden).
- Gelb – Das Ziel ist "down" (aus), jedoch "connected" (verbunden).
- Rot – Das Ziel ist "down/idle" (aus/inaktiv), "busy" (belegt) oder aus anderen Gründen nicht verfügbar.

Diese Funktion ist vom Virtual KVM Client (VKC), vom Active KVM Client (AKC) und vom Multi-Platform-Client (MPC) verfügbar.

Hinweis: Der MPC verwendet eine andere Methode zum Initiieren eines Scans als die anderen Raritan-Clients. Details hierzu finden Sie im Benutzerhandbuch ***KVM and Serial Client Guide*** *unter* ***Set Scan Group*** *(Scangruppe einstellen). Die Remotekonsole und die lokale Konsole weisen unterschiedliche Scanergebnisse und Scanoptionen auf. Siehe* **Scannen von Ports – Lokale Konsole** *(auf Seite 207).*

So suchen Sie nach Zielen:

1. Klicken Sie auf der Seite "Port Access" (Portzugriff) auf die Registerkarte "Set Scan" (Scanfunktion einstellen).
2. Wählen Sie die Ziele aus, die in die Suche einbezogen werden sollen, indem Sie das Kontrollkästchen links neben dem jeweiligen Ziel aktivieren. Durch Aktivieren des Kontrollkästchens oben in der Zielspalte können Sie auch alle Ziele auswählen.
3. Lassen Sie das Kontrollkästchen "Up Only" (Nur ein) aktiviert, wenn nur Ziele in die Suche einbezogen werden sollen, die eingeschaltet sind. Deaktivieren Sie dieses Kontrollkästchen, wenn Sie alle Ziele, egal ob ein- oder ausgeschaltet, in die Suche einbeziehen möchten.
4. Klicken Sie auf "Scan" (Scannen), um die Suche zu starten. Jedes gescannte Ziel wird in einer Bildschirmpräsentation auf der Seite angezeigt.
5. Klicken Sie auf "Options" (Optionen) > "Pause" (Pausieren), um die Bildschirmpräsentation anzuhalten und nicht mehr zwischen Zielen zu wechseln. Klicken Sie auf "Options" (Optionen) > "Resume" (Fortsetzen), um die Bildschirmpräsentation fortzusetzen.
6. Klicken Sie auf die Miniaturansicht eines Ziels, um es als Nächstes zu scannen.
7. Stellen Sie eine Verbindung zu einem Ziel her, indem Sie auf die zugehörige Miniaturansicht doppelklicken.

View By Port | Set Scan

▲ No.	Name	Type	Status	Availability
1	Dominion_LX_Port1	Not Available	down	idle
2	Dominion_LX_Port2	Not Available	down	idle
3	Dominion_LX_Port3	Not Available	down	idle
4	Dominion_LX_Port4	Not Available	down	idle
5	Dominion_LX_Port5	Not Available	down	idle
6	Dominion_LX_Port6	Not Available	down	idle
7	Dominion_LX_Port7	Not Available	down	idle
8	Dominion_LX_Port8	Not Available	down	idle
9	Dominion_LX_Port9	Not Available	down	idle
10	[illegible]	[illegible]	[illegible]	idle



Verwenden von Scanoptionen

Die folgenden Optionen sind beim Scannen von Zielen verfügbar. Mit Ausnahme des Symbols "Expand/Collapse" (Erweitern/Reduzieren) können alle Optionen im Menü "Options" (Optionen) oben links in der Anzeige "Port Scan" (Port-Scan) ausgewählt werden. Beim Schließen des Fensters werden die Optionen auf die Standardeinstellungen zurückgesetzt.

Ausblenden oder Anzeigen von Miniaturansichten

- Mit dem Symbol "Expand/Collapse" (Erweitern/Reduzieren) oben links im Fenster können Sie Miniaturansichten ausblenden und anzeigen. Die erweiterte Ansicht ist die Standardeinstellung.

Pausieren der Bildschirmpräsentation von Miniaturansichten

- Unterbrechen Sie den Wechsel der Miniaturansichten zwischen einem Ziel und dem nächsten, indem Sie "Options" (Optionen) > "Pause" (Pausieren) auswählen. In der Standardeinstellung wird zwischen den Miniaturansichten gewechselt.

Pausieren der Bildschirmpräsentation von Miniaturansichten

- Setzen Sie den Wechsel zwischen den Miniaturansichten durch Auswählen von "Options" (Optionen) > "Resume" (Fortsetzen) fort.

Anpassen der Größe von Miniaturansichten in der Anzeige "Port Scan" (Port-Scan)

- Vergrößern Sie die Miniaturansichten, indem Sie "Options" (Optionen) > "Size" (Größe) > "360x240" auswählen.
- Zum Verkleinern der Miniaturansichten wählen Sie "Options" (Optionen) > "Size" (Größe) > "160x120" aus. Dies ist die Standardgröße für Miniaturansichten.

Ändern der Ausrichtung der Anzeige "Port Scan" (Port-Scan)

- Zum Anzeigen der Miniaturansichten am unteren Rand der Anzeige "Port Scan" (Port-Scan) wählen Sie "Options" (Optionen) > "Split Orientation" (Ausrichtung teilen) > "Horizontal".
- Zum Anzeigen der Miniaturansichten rechts in der Anzeige "Port Scan" (Port-Scan) wählen Sie "Options" (Optionen) > "Split Orientation" (Ausrichtung teilen) > "Vertical" (Vertikal). Dies ist die Standardansicht.

Verwalten von Favoriten

Mithilfe des Features "Favorites" (Favoriten) können Sie die häufig verwendeten Geräte organisieren und schnell darauf zugreifen. Der Bereich "Favorite Devices" (Bevorzugte Geräte) befindet sich links unten (Randleiste) auf der Seite "Port Access" (Port-Zugriff). Hier haben Sie folgende Möglichkeiten:

- Erstellen und Verwalten einer Liste bevorzugter Geräte
- Schnelles Zugreifen auf häufig verwendete Geräte
- Auflisten der Favoriten nach Gerätename, IP-Adresse oder DNS-Hostname
- Erkennen von LX-Geräten im Subnetz (vor und nach der Anmeldung)
- Abrufen erkannter LX-Geräte vom verbundenen Dominion-Gerät (nach der Anmeldung)

So greifen Sie auf ein bevorzugtes LX-Gerät zu:

- Klicken Sie auf den unterhalb von "Favorite Devices" (Bevorzugte Geräte) aufgeführten Namen des Geräts. Ein neues Browserfenster wird geöffnet.

So zeigen Sie die Favoriten nach Name an:

- Klicken Sie auf "Display by Name" (Nach Name anzeigen).

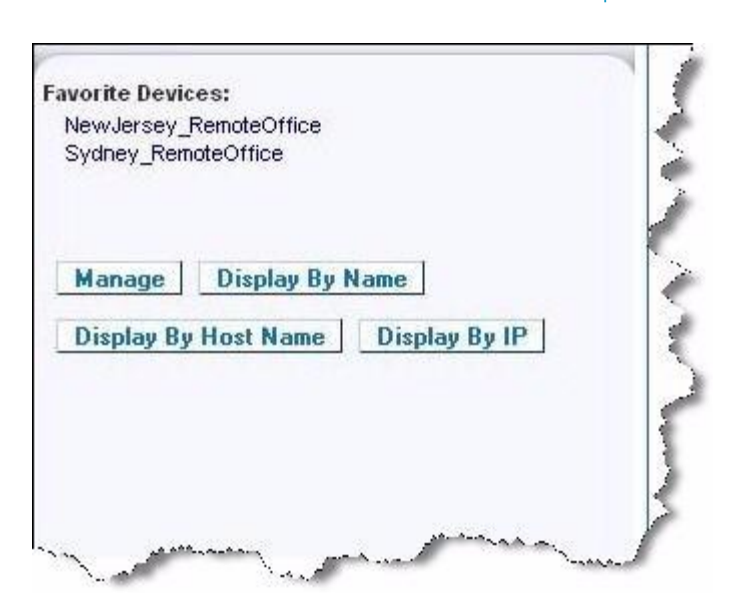
So zeigen Sie die Favoriten nach IP-Adresse an:

- Klicken Sie auf "Display by IP" (Nach IP anzeigen).

So zeigen Sie die Favoriten nach Hostname an:

- Klicken Sie auf "Display by Host Name" (Nach Hostname anzeigen).





Seite "Manage Favorites" (Favoriten verwalten)

So öffnen Sie die Seite "Manage Favorites" (Favoriten verwalten):

- Klicken Sie auf die Schaltfläche "Manage" (Verwalten) im linken Bildschirmbereich. Die Seite "Manage Favorites" (Favoriten verwalten) wird angezeigt. Diese Seite enthält die folgenden Optionen:

Option	Aktion
"Favorites List" (Favoritenliste)	Verwalten einer Liste bevorzugter Geräte
"Discover Devices - Local Subnet" (Geräte erkennen – Lokales Subnetz)	Erkennen von Raritan-Geräten auf dem lokalen Subnetz des Client-PC.
"Discover Devices - LX Subnet" (Geräte erkennen – LX-Subnetz)	Erkennen der Raritan-Geräte im Subnetz des LX-Geräts
"Add New Device to Favorites" (Neues Gerät zu Favoriten hinzufügen)	Hinzufügen, Bearbeiten und Löschen von Geräten in der Favoritenliste

Seite "Favorites List" (Favoritenliste)

Auf der Seite "Favorites List" (Favoritenliste) können Sie der Favoritenliste Geräte hinzufügen und in der Favoritenliste aufgeführte Geräte bearbeiten oder löschen.

So öffnen Sie die Seite "Favorites List" (Favoritenliste):

- Wählen Sie "Manage > Favorites List" (Verwalten > Favoritenliste). Die Seite "Favorites List" (Favoritenliste) wird angezeigt.

Erkennen von Geräten auf dem lokalen Subnetz

Mit dieser Option werden die Geräte auf dem lokalen Subnetz erkannt. Dieses ist das Subnetz, auf dem die LX-Remotekonsole ausgeführt wird. Auf die Geräte können Sie direkt von dieser Seite aus zugreifen, oder Sie können sie zur Favoritenliste hinzufügen. Siehe***Seite "Favorites List"*** (siehe "***Seite "Favorites List" (Favoritenliste)***" auf Seite 56) (Favoritenliste).

So finden Sie Geräte im lokalen Subnetz:

1. Wählen Sie "Manage" > "Discover Devices – Local Subnet" (Verwalten > Geräte erkennen – Lokales Subnetz) aus. Die Seite "Discover Devices – Local Subnet" (Geräte erkennen – Lokales Subnetz) wird angezeigt.
2. Wählen Sie den entsprechenden Erkennungsport aus:
   - Wenn Sie den Standarderkennungs-Port verwenden möchten, aktivieren Sie das Kontrollkästchen "Use Default Port 5000" (Standard-Port 5000 verwenden).
   - Wenn Sie einen anderen Erkennungs-Port verwenden möchten, gehen Sie wie folgt vor:

   a. Deaktivieren Sie das Kontrollkästchen "Use Default Port 5000" (Standard-Port 5000 verwenden).

   b. Geben Sie die Portnummer im Feld "Discover on Port" (Erkennungsport) ein.

   c. Klicken Sie auf "Save" (Speichern).
3. Klicken Sie auf "Refresh" (Aktualisieren). Die Liste der Geräte im lokalen Subnetz wird aktualisiert.

So fügen Sie der Favoritenliste Geräte hinzu:

1. Aktivieren Sie das Kontrollkästchen neben dem gewünschten Gerätenamen/der IP-Adresse.
2. Klicken Sie auf "Add" (Hinzufügen).



So greifen Sie auf ein erkanntes Gerät zu:

- Klicken Sie auf den Gerätenamen oder die IP-Adresse des Geräts. Ein neues Browserfenster wird geöffnet.

Erkennen von Geräten auf dem LX-Subnetz

Mit dieser Option werden Geräte auf dem Gerätesubnetz erkannt. Dieses ist das Subnetz der Geräte-IP-Adresse von LX. Auf die Geräte können Sie direkt von der Subnetzseite aus zugreifen, oder Sie können sie zur Favoritenliste hinzufügen. Siehe***Seite "Favorites List"*** (siehe "***Seite "Favorites List" (Favoritenliste)***" auf Seite 56) (Favoritenliste).

Mit diesem Feature arbeiten mehrere LX-Geräte zusammen und werden automatisch skaliert. Die LX-Remotekonsole erkennt die LX-Geräte und alle sonstigen Raritan-Geräte im LX-Subnetz automatisch.

So finden Sie Geräte im Subnetz des Geräts:

1. Wählen Sie Manage > Discover Devices – LX Subnet (Verwalten > Geräte erkennen – LX-Subnetz) aus. Die Seite "Discover Devices – LX Subnet" (Geräte erkennen – LX-Subnetz) wird angezeigt.
2. Klicken Sie auf "Refresh" (Aktualisieren). Die Liste der Geräte im lokalen Subnetz wird aktualisiert.

So fügen Sie der Favoritenliste Geräte hinzu:

1. Aktivieren Sie das Kontrollkästchen neben dem gewünschten Gerätenamen/der IP-Adresse.
2. Klicken Sie auf "Add" (Hinzufügen).

So greifen Sie auf ein erkanntes Gerät zu:

- Klicken Sie auf den Gerätenamen oder die IP-Adresse des Geräts. Ein neues Browserfenster wird geöffnet.

Hinzufügen, Löschen und Bearbeiten der Favoriten

So fügen Sie der Favoritenliste ein Gerät hinzu:

1. Wählen Sie "Manage" > "Add New Device to Favorites" (Verwalten > Neues Gerät zu Favoriten hinzufügen) aus. Die Seite "Add New Favorite" (Neuen Favoriten hinzufügen) wird angezeigt.
2. Geben Sie eine aussagekräftige Beschreibung ein.
3. Geben Sie die IP-Adresse/den Hostnamen des Geräts ein.
4. Ändern Sie ggf. den Erkennungs-Port.
5. Wählen Sie die Produktart aus.
6. Klicken Sie auf "OK". Das Gerät wird Ihrer Favoritenliste hinzugefügt.

So bearbeiten Sie einen Favoriten:

1. Aktivieren Sie auf der Seite "Favorites List" (Favoritenliste) das Kontrollkästchen neben dem gewünschten LX-Gerät.
2. Klicken Sie auf "Edit" (Bearbeiten). Die Seite "Edit" (Bearbeiten) wird angezeigt.
3. Aktualisieren Sie die Felder nach Bedarf:
   - Beschreibung
   - IP Address/Host Name (IP-Adresse/Hostname) – Geben Sie die IP-Adresse des LX-Geräts ein.
   - Port (falls erforderlich)
   - Product Type (Produktart)
4. Klicken Sie auf "OK".

So löschen Sie einen Favoriten:

Wichtig: Gehen Sie beim Löschen von Favoriten sorgfältig vor. Sie werden nicht aufgefordert, den Löschvorgang zu bestätigen.

1. Aktivieren Sie das Kontrollkästchen neben dem gewünschten LX-Gerät.
2. Klicken Sie auf "Delete" (Löschen). Der Favorit wird aus der Favoritenliste entfernt.

Abmelden

So beenden Sie LX:

- Klicken Sie oben rechts auf der Seite auf "Logout" (Abmelden).

Hinweis: Durch das Abmelden werden auch alle geöffneten Sitzungen von Virtual KVM Client und des seriellen Clients geschlossen.

Proxyserverkonfiguration für die Verwendung mit MPC, VKC und AKC

Wenn ein Proxyserver verwendet werden muss, muss ein SOCKS-Proxy bereitstehen und auf dem Remote-Client-PC konfiguriert werden.

Hinweis: Wenn der installierte Proxyserver nur das HTTP-Proxyprotokoll unterstützt, können Sie keine Verbindung herstellen.

So konfigurieren Sie den SOCKS-Proxy:

1. Wählen Sie auf dem Client "Control Panel > Internet Options" (Systemsteuerung > Internetoptionen) aus.



a. Klicken Sie auf der Registerkarte "Connections" (Verbindungen) auf "LAN settings" (LAN-Einstellungen). Das Dialogfeld "Local Area Network (LAN) Settings" (LAN-Einstellungen) wird geöffnet.

b. Wählen Sie "Use a proxy server for your LAN" (Proxyserver für LAN verwenden) aus.

c. Klicken Sie auf "Advanced" (Erweitert). Das Dialogfeld "Proxy Settings" (Proxyeinstellungen) wird angezeigt.

d. Konfigurieren Sie die Proxyserver für alle Protokolle. WICHTIG: Wählen Sie nicht "Use the same proxy server for all protocols" (Denselben Proxyserver für alle Protokolle verwenden) aus.

Hinweis: Der Standardport für ein SOCKS-Proxy (1080) unterscheidet sich vom HTTP-Proxy (3128).

---

2. Klicken Sie in jedem Dialogfeld auf "OK", um die Einstellungen zu übernehmen.

3. Konfigurieren Sie anschließend die Proxys für die Java™-Applets, indem Sie "Control Panel > Java" (Systemsteuerung > Java) auswählen.

e. Klicken Sie auf der Registerkarte "General" (Allgemein) auf "Network Settings" (Netzwerkeinstellungen). Das Dialogfeld "Network Settings" (Netzwerkeinstellungen) wird angezeigt.

f. Wählen Sie "Use Proxy Server" (Proxyserver verwenden) aus.

g. Klicken Sie auf "Advanced" (Erweitert). Das Dialogfeld "Advanced Network Settings" (Erweiterte Netzwerkeinstellungen) wird angezeigt.

h. Konfigurieren Sie die Proxyserver für alle Protokolle. WICHTIG: Wählen Sie nicht "Use the same proxy server for all protocols" (Denselben Proxyserver für alle Protokolle verwenden) aus.

Hinweis: Der Standardport für ein SOCKS-Proxy (1080) unterscheidet sich vom HTTP-Proxy (3128).

---

4. Wenn Sie ein Standalone-MPC verwenden, müssen Sie folgende Schritte ausführen:

i. Öffnen Sie die Datei "start.bat" im MPC-Verzeichnis in einem Texteditor.

j. Fügen Sie die folgenden Parameter in die Befehlszeile ein. Fügen Sie sie vor "-classpath" ein: -DsocksProxyHost=<socks proxy ip addr> -DsocksProxyPort=<socks proxy port>

Die Parameter müssen wie folgt aussehen:

start javaw -Xmn128M -Xmx512M -XX:MaxHeapFreeRatio=70 -
XX:MinHeapFreeRatio=50 -Dsun.java2d.noddraw=true -
DsocksProxyHost=192.168.99.99 -DsocksProxyPort=1080 -
classpath .\sdeploy.jar;.\sFoxtrot.jar;.\jaws.jar;.\sMpc.jar
com.raritan.rrc.ui.RRCApplication %1



Virtual KVM Client (VKC) und Active KVM Client (AKC)

Der Virtual KVM Client (VKC) und der Active KVM Client (AKC) sind Schnittstellen, mit denen auf Remoteziele zugegriffen werden kann. Der AKC und VKC verfügen mit Ausnahme der nachfolgend aufgeführten Punkte über identische Leistungsmerkmale:

- Mindestanforderungen an das System
- Unterstützte Betriebssysteme und Browser
- Auf dem AKC erstellte Tastaturmakros können im VKC nicht genutzt werden.
- Konfiguration des direkten Portzugriffs (siehe **Aktivieren des direkten Port-Zugriffs über URL** (auf Seite 145))
- Konfiguration der AKC-Serverzertifikat-Validierung (siehe **Voraussetzungen für die Verwendung des AKC**)

Informationen zum Raritan Virtual KVM Client

Wenn Sie über die Remotekonsole auf einen Zielserver zugreifen, wird ein Fenster für den Virtual KVM Client (VKC) geöffnet. Es steht ein Virtual KVM Client für jeden verbundenen Zielserver zur Verfügung. Auf diese Fenster kann über die Windows®-Taskleiste zugegriffen werden.

Hinweis: Einige Funktionen wie zum Beispiel die Starteinstellungen für den Client und Smart Cards werden von LX nicht unterstützt und werden deshalb auch nicht vom AKC oder VKC unterstützt, wenn sie zusammen mit LX verwendet werden.

Hinweis: Der KX II-101-V2 unterstützt nur eine Verbindung zu jeweils einem Ziel.

Die Fenster des Virtual KVM Client können minimiert, maximiert und auf dem Desktop verschoben werden.

Hinweis: Beachten Sie, dass beim Aktualisieren des HTML-Browsers die Verbindung des Virtual KVM Client beendet wird.

Hinweis: Wenn Sie Firefox 3.0.3 verwenden, kann es zu Problemen beim Starten der Anwendung kommen. Wenn dies der Fall ist, löschen Sie den Browser-Cache und starten Sie die Anwendung erneut.



Informationen zum Active KVM Client

Der AKC basiert auf Microsoft Windows .NET-Technologie. Sie können den Client in Windows-Umgebungen ausführen, ohne die Java Runtime Environment (JRE) zu verwenden, welche zur Ausführung des Virtual KVM Client (VKC) und des Multi-Platform-Client (MPC) von Raritan erforderlich ist.

Hinweis: Einige Funktionen wie zum Beispiel die Starteinstellungen für den Client und Smart Cards werden von LX nicht unterstützt und werden deshalb auch nicht vom AKC oder VKC unterstützt, wenn sie zusammen mit LX verwendet werden.

Vom AKC unterstützte .NET Framework-Versionen, Betriebssysteme und Browser

.NET Framework

Der AKC benötigt Windows .NET® Version 3.5 und funktioniert mit Version 3.5 und Version 4.0, jedoch nicht allein mit Version 4.0.

Betriebssysteme

Wurde der AKC über Internet Explorer® gestartet, bietet er Ihnen die Möglichkeit, über KX II 2.2 (und höher) und LX 2.4.5 (und höher) auf Zielserver zuzugreifen. Der AKC ist mit den folgenden Plattformen kompatibel, auf denen .NET Framework 3.5 ausgeführt wird:

- Windows XP®-Betriebssystem
- Windows Vista®-Betriebssystem (bis 64 Bit)
- Windows Vista®-Betriebssystem (bis 64 Bit)

Da .NET für die Ausführung von AKC benötigt wird, erhalten Sie, wenn Sie .NET nicht oder eine nicht unterstützte Version von .NET installiert haben, eine Meldung, in der Sie aufgefordert werden, die Version von .NET zu prüfen.

Browser

- Internet Explorer 6 oder höher

Wenn Sie versuchen, den AKC über einem anderen Browser als IE 6 oder höher zu öffnen, wird Ihnen eine Fehlermeldung angezeigt, in der Sie aufgefordert werden, zu prüfen, welchen Browser Sie verwenden und ggf. Internet Explorer zu verwenden.

Voraussetzungen für die Verwendung des AKC

So verwenden Sie den AKC:

- Stellen Sie sicher, dass die Cookies von der IP-Adresse des Geräts, auf das zugegriffen wird, nicht blockiert werden.
- Die Benutzer von Windows Vista-, Windows 7- und Windows 2008-Servern müssen sicherstellen, dass die IP-Adresse des Geräts, auf das zugegriffen wird, in der Zone "Vertrauenswürdige Sites" hinzugefügt wurde und dass der "Geschützte Modus" nicht aktiv ist, wenn auf das Gerät zugegriffen wird.

Enable AKC Download Server Certificate Validation (AKC-Download-Serverzertifikat-Validierung aktivieren)

Falls durch den Geräteadministrator die Option "Enable AKC Download Server Certificate Validation" (AKC-Download-Serverzertifikat-Validierung aktivieren) aktiviert wurde:

- Administratoren müssen ein gültiges Zertifikat auf das Gerät hochladen oder ein selbstsigniertes Zertifikat auf dem Gerät generieren. Das Zertifikat muss über eine gültige Hostbezeichnung verfügen.
- Jeder Benutzer muss das CA-Zertifikat (oder eine Kopie des selbstsignierten Zertifikats) zum Speicher für "Vertrauenswürdige Stammzertifizierungsstellen" seines Browsers hinzufügen.

Symbolleiste

Schaltfläche	Schaltflächenname	Beschreibung
	Properties (Eigenschaften)	Öffnet das Dialogfeld "Modify Connection Properties" (Verbindungseigenschaften bearbeiten), über das Sie die Bandbreitenoptionen (z. B. Verbindungsgeschwindigkeit, Farbtiefe usw.) manuell anpassen können.
	Video Settings (Videoeinstellungen)	Öffnet das Dialogfeld "Video Settings" (Videoeinstellungen), über das Sie die Videokonvertierungsparameter manuell anpassen können.
	Color Calibration (Farbkalibrierung)	Dient zum Anpassen der Farbeinstellungen, um überflüssiges Farbrauschen zu reduzieren. Diese Option ist identisch mit der Auswahl von "Video" > "Color Calibrate" (Video > Farbkalibrierung). *Hinweis: Nicht verfügbar für KX II-101-V2.*



Schaltfläche	Schaltflächenname	Beschreibung
	Target Screenshot (Screenshot des Zielgeräts)	Klicken Sie auf diese Option, um einen Screenshot des Zielservers aufzunehmen und diesen in einer Datei Ihrer Wahl zu speichern.
	Audio	Öffnet ein Dialogfeld, in dem Sie aus einer Liste von Audiogeräten, die an einen Client-PC angeschlossen sind, auswählen können. Nachdem Audiogeräte mit dem Ziel verbunden wurden, können Sie die Verbindung der Geräte durch Auswahl dieser Option trennen. *Hinweis: Diese Funktion ist im KX II 2.4.0 (und höher) verfügbar.* *Hinweis: Diese Funktion wird von LX nicht unterstützt.*
	Synchronize Mouse (Maus synchronisieren)	Zwei-Cursor-Modus erzwingt die erneute Ausrichtung des Zielservercursors mit dem Cursor. *Hinweis: Nicht verfügbar für KX II-101-V2.*
	Refresh Screen (Anzeige aktualisieren)	Aktualisiert den Videobildschirm.
	Auto-sense Video Settings (Videoeinstellungen automatisch erkennen)	Aktualisiert die Videoeinstellungen (Auflösung, Aktualisierungsfrequenz).
	"Smart Card"	Öffnet ein Dialogfeld, in dem Sie aus einer Liste von Smart Card-Lesegeräten, die an einen Client-PC angeschlossen sind, auswählen können. *Hinweis: Diese Funktion ist im KSX II 2.3.0 (und höher) und im KX II 2.1.10 (und höher) verfügbar.* *Hinweis: Diese Funktion wird von LX nicht unterstützt.*

Schaltfläche	Schaltflächenname	Beschreibung
	Send Ctrl+Alt+Delete (Strg+Alt+Entf senden)	Sendet die Tastenkombination "Strg+Alt+Entf" an den Zielserver.
	Single Cursor Mode (Ein-Cursor-Modus)	Startet den Ein-Cursor-Modus, bei dem der lokale Cursor nicht mehr auf dem Bildschirm angezeigt wird. Drücken Sie Strg+Alt+O, um diesen Modus zu beenden. *Hinweis: Nicht verfügbar für KX II-101-V2.*
	Vollbildmodus	Maximiert die Anzeige des Zielserverdesktops, so dass er auf dem gesamten Bildschirm angezeigt wird.
	Scaling (Skalieren)	Vergrößert oder verkleinert die Zielvideogröße, sodass Sie den gesamten Inhalt des Zielserverfensters anzeigen können, ohne die Bildlaufleiste verwenden zu müssen.

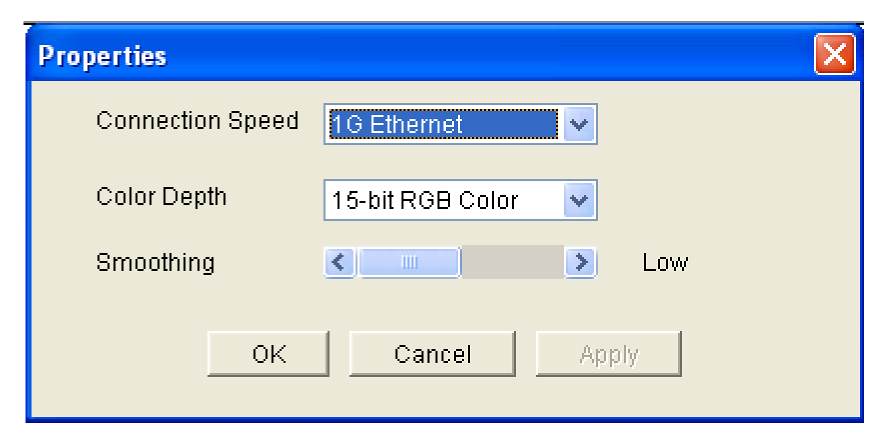
Properties (Eigenschaften)

Die dynamischen Videokomprimierungsalgorithmen gewährleisten die Verwendbarkeit der KVM-Konsole unter variierenden Bandbreitenbeschränkungen. Die Geräte optimieren die KVM-Ausgabe nicht nur für LAN-, sondern auch für WAN-Verbindungen. Diese Geräte können zudem die Farbtiefe steuern und die Videoausgabe beschränken, um für jede Bandbreite ein optimales Gleichgewicht zwischen Videoqualität und Systemreaktion bereitzustellen.

Sie können die Parameter im Dialogfeld "Properties" (Eigenschaften) Ihren Anforderungen für unterschiedliche Betriebsumgebungen anpassen. Einmal vorgenommene und gespeicherte Verbindungseigenschaften werden auch für spätere Verbindungen zu Geräten der 2. Generation gespeichert.

So legen Sie die Verbindungseigenschaften fest:

1. Wählen Sie "Connection" > "Properties" (Verbindung > Eigenschaften) oder klicken Sie auf die Schaltfläche "Connection Properties" (Verbindungseigenschaften) in der Symbolleiste. Das Dialogfeld "Properties" (Eigenschaften) wird angezeigt.



Hinweis: 1G Ethernet wird vom KX II-101 nicht unterstützt.

2. Wählen Sie in der Dropdownliste "Connection Speed" (Verbindungsgeschwindigkeit) die gewünschte Verbindungsgeschwindigkeit aus. Das Gerät kann die verfügbare Bandbreite automatisch erkennen und die Bandbreitenverwendung nicht beschränken. Sie können diese Verwendung jedoch auch gemäß den Bandbreitenbeschränkungen anpassen.
   - Automatisch
   - 1G Ethernet
   - 100 MB Ethernet
   - 10 MB Ethernet

- 1,5 MB (MAX DSL/T1)
- 1 MB (Schnelles DSL/T1)
- 512 KB (Mittleres DSL/T1)
- 384 KB (Langsames DSL/T1)
- 256 KB (Kabel)
- 128 KB (Dual-ISDN)
- 56 KB (ISP-Modem)
- 33 KB (Schnelles Modem)
- 24 KB (Langsames Modem)

Diese Einstellungen sind nicht als genaue Geschwindigkeitsangaben zu verstehen, sondern als Optimierungen für bestimmte Bedingungen. Der Client und der Server versuchen stets, Videodaten so schnell wie möglich über das Netzwerk zu übertragen, unabhängig von der aktuellen Netzwerkgeschwindigkeit und Codierungseinstellung. Das System arbeitet jedoch am schnellsten, wenn die Einstellungen der tatsächlichen Umgebung entsprechen.

3. Wählen Sie in der Dropdownliste "Color Depth" (Farbtiefe) die gewünschte Farbtiefe aus. Das Gerät kann die an Remotebenutzer übertragene Farbtiefe dynamisch anpassen, um die Verwendbarkeit in allen Bandbreiten zu maximieren.
   - 15-Bit-Farbe (RGB)
   - 8-Bit-Farbe (RGB)
   - 4-Bit-Farbe
   - 4-Bit-Graustufen
   - 3-Bit-Graustufen
   - 2-Bit-Graustufen
   - Schwarzweiß

Wichtig: Für die meisten Verwaltungsaufgaben (Überwachung, erneute Konfiguration von Servern usw.) wird das von den modernen Videografikkarten bereitgestellte vollständige 24-Bit- oder 32-Bit-Farbspektrum nicht benötigt. Durch den Versuch, solch hohe Farbtiefen zu übertragen, wird Netzwerkbandbreite verschwendet.

---

4. Verwenden Sie den Schieberegler um die gewünschte Glättung auszuwählen (nur im 15-Bit-Farbmodus). Die Glättungsebene bestimmt, wie stark Bildschirmbereiche mit geringer Farbvariation zu einer einheitlichen Farbe zusammengefasst werden. Die Glättung verbessert das Aussehen des Zielgerätbildes, da dadurch das Videorauschen verringert wird.
5. Klicken Sie auf OK, um die Eigenschaften festzulegen.



Verbindungsinformationen

So erhalten Sie Informationen über die Verbindung des Virtual KVM Client:

- Wählen Sie "Connection > Info..." (Verbindung > Info...). Das Fenster "Connection Info" (Verbindungsinformationen) wird angezeigt.

Zur aktuellen Verbindung werden folgende Informationen angezeigt:

- Device Name (Gerätename) – Der Name des Geräts.
- IP-Address (IP-Adresse) – Die IP-Adresse des Geräts.
- Port – Der TCP/IP-Port für die KVM-Kommunikation, über den auf das Zielgerät zugegriffen wird.
- Data In/Second (Dateneingang/Sekunde) – Eingehende Datenrate.
- Data Out/Second (Datenausgang/Sekunde) – Ausgehende Datenrate.
- Connect Time (Verbindungsdauer) – Die Dauer der Verbindung.
- FPS – Frames pro Sekunde der übertragenen Videobilder.
- Horizontal Resolution (Horizontale Auflösung) – Die horizontale Bildschirmauflösung.
- Vertical Resolution (Vertikale Auflösung) – Die vertikale Bildschirmauflösung.
- Refresh Rate (Aktualisierungfrequenz) – Gibt an, wie häufig die Anzeige aktualisiert wird.
- Protocol Version (Protokollversion) – Die RFB-Protokollversion.

So kopieren Sie diese Informationen:

- Klicken Sie auf "Copy to Clipboard" (In Zwischenablage kopieren). Anschließend können die Informationen in ein Programm Ihrer Wahl eingefügt werden.

Tastaturoptionen

Keyboard Macros (Tastaturmakros)

Tastaturmakros gewährleisten, dass für den Zielserver vorgesehene Tastenkombinationen an den Zielserver gesendet und nur von diesem interpretiert werden. Andernfalls werden sie von dem Computer interpretiert, auf dem der Virtual KVM Client ausgeführt wird (Client-PC).

Makros werden auf dem Client-PC gespeichert und sind PC-spezifisch. Wenn Sie einen anderen PC verwenden, können Sie daher Ihre Makros nicht sehen. Wenn eine andere Person Ihren PC verwendet und sich mit einem anderen Benutzernamen anmeldet, werden ihr die Makros angezeigt, da sie für den gesamten Computer gelten.

Im Virtual KVM Client erstellte Tastaturmakros stehen im Multi-Platform Client (MPC) zur Verfügung und umgekehrt. Tastaturmakros, die auf dem Active KVM Client (AKC) erstellt wurden, können jedoch nicht in VKC oder MPC verwendet werden. Dies trifft umgekehrt ebenfalls zu.

Hinweis: AKC wird nicht von KX II-101 unterstützt.

Tastaturmakros importieren/exportieren

Makros, die von dem Active KVM Client (AKC) exportiert wurden, können nicht in einen Multi-Platform Client (MPC) oder Virtual KVM Client (VKC) importiert werden. Von MPC oder VKC exportierte Makros können nicht in AKC importiert werden.

Hinweis: AKC wird nicht von KX II-101 unterstützt.

► **So importieren Sie Makros:**

1. Zum Öffnen des Dialogfelds "Import Macros" (Makros importieren) wählen Sie "Keyboard > Import Keyboard Macros" (Tastatur > Tastaturmakros importieren). Navigieren Sie zu dem Ordner, in dem die Makrodatei abgespeichert ist.
2. Klicken Sie auf die Makrodatei und anschließend auf "Open" (Öffnen), um das Makro zu importieren.
    a. Wenn zu viele Makros in der Datei enthalten sind, wird eine Fehlermeldung angezeigt. Wenn Sie auf "OK" klicken, wird der Import abgebrochen.
    b. Schlägt der Import fehl, wird ein Dialogfeld "Error" (Fehler) und eine Meldung mit den Gründen für den fehlgeschlagenen Import angezeigt. Klicken Sie auf "OK" und setzen Sie den Import fort, ohne dabei jedoch die Makros zu importieren, bei denen der Import fehlgeschlagen ist.

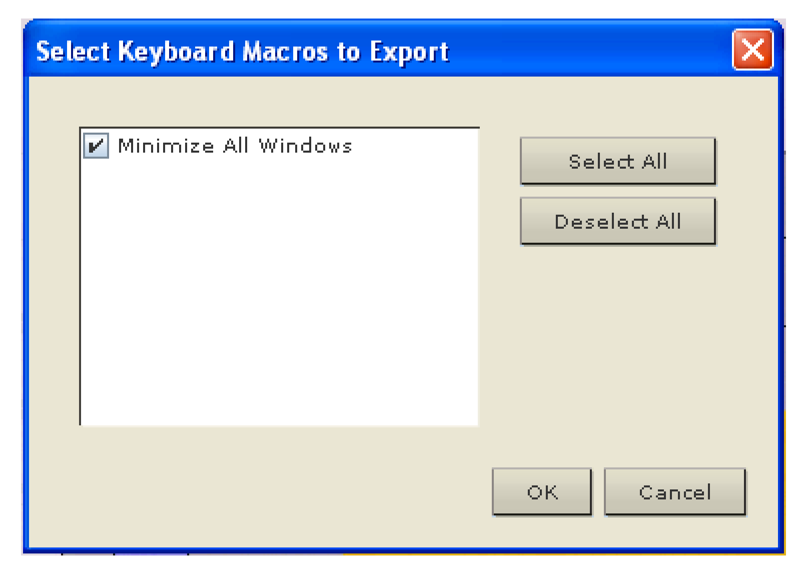


3. Wählen Sie die zu importierenden Makros aus, indem Sie die entsprechenden Kontrollkästchen markieren, oder verwenden Sie die Option "Select All" (Alle auswählen) bzw. "Deselect All" (Alle deaktivieren).
4. Klicken Sie auf "OK", um den Import zu starten.
   a. Wird ein doppelt vorhandenes Makro gefunden, wird das Dialogfeld "Import Macros" (Makros importieren) angezeigt. Führen Sie einen der folgenden Schritt aus:
      - Klicken Sie auf "Yes" (Ja), um das bereits vorhandene Makro mit dem importierten zu ersetzen.
      - Klicken Sie auf "Yes to All" (Ja, alle), um die jeweils ausgewählten sowie alle anderen gefundenen doppelten Makros zu ersetzen.
      - Klicken Sie auf "No" (Nein), um das ursprüngliche Makro beizubehalten, und fahren Sie dann mit dem nächsten Makro fort.
      - Klicken Sie auf "No to All" (Nein, nicht alle), um das ursprüngliche Makro beizubehalten, und fahren Sie dann mit dem nächsten Makro fort. Werden weitere doppelte Makros gefunden, werden diese bei dem Vorgang ebenfalls übergangen.
      - Klicken Sie auf "Cancel" (Abbrechen), um den Import abzubrechen.
      - Sie können ebenfalls auf "Rename" (Umbenennen) klicken, um das Makro umzubenennen und es dann zu importieren. Wenn Sie "Rename" (Umbenennen) ausgewählt haben, wird das Dialogfeld "Rename Macro" (Makro umbenennen) angezeigt. Geben Sie in das Feld einen neuen Namen für das Makro ein und klicken Sie auf "OK". Das Dialogfeld wird geschlossen und der Vorgang wird fortgesetzt. Wenn es sich bei dem eingegebenen Namen um den eines doppelten Makros handelt, wird eine Warnmeldung angezeigt und Sie werden aufgefordert, einen anderen Namen für den Makro einzugeben.
   b. Wenn während des Importprozesses die erlaubte Anzahl von importierten Makros überstiegen wird, wird ein Dialogfeld angezeigt. Klicken Sie auf "OK", wenn Sie den Importvorgang der Makros fortsetzen möchten, oder klicken Sie auf "Cancel" (Abbrechen), um den Vorgang zu beenden.

Die Makros werden dann importiert. Wenn ein Makro importiert wird, das eine bereits vorhandene Zugriffstaste enthält, wird die Zugriffstaste für das importierte Makro verworfen.

So exportieren Sie Makros:

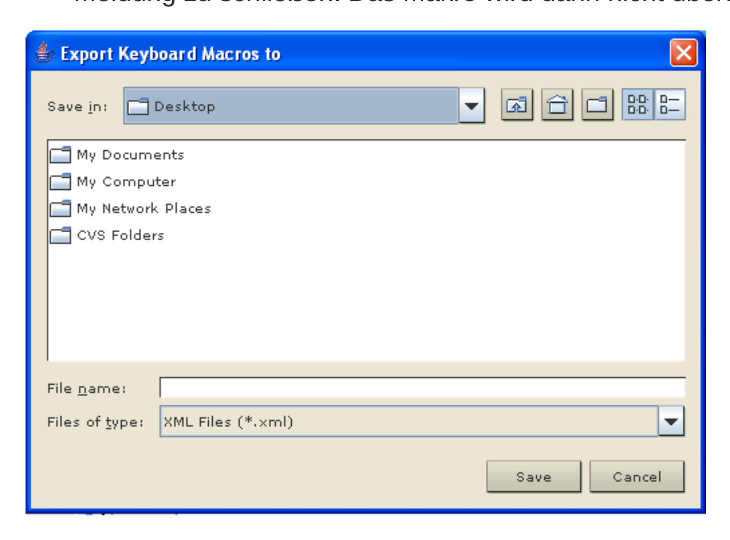
1. Um das Dialogfeld "Select Keyboard Macros to Export" (Tastaturmakros für den Export auswählen) zu öffnen, wählen Sie "Tools > Export Macros" (Extras > Makros exportieren) aus.



2. Wählen Sie die zu exportierenden Makros aus, indem Sie die entsprechenden Kontrollkästchen markieren, oder verwenden Sie die Option "Select All" (Alle auswählen) bzw. "Deselect All" (Alle deaktivieren).
3. Klicken Sie auf "OK". Hier können Sie die gewünschte Makrodatei auswählen. Das Makro ist standardmäßig auf Ihrem Desktop vorhanden.



4. Wählen Sie den Ordner aus, in dem Sie die Makrodatei abspeichern möchten, geben Sie einen Namen für die Datei ein und klicken Sie auf "Save" (Speichern). Wenn das Makro bereits vorhanden ist, wird eine Warnmeldung angezeigt. Klicken Sie auf "Yes" (Ja), um das vorhandene Makro zu überschreiben, oder auf "No" (Nein), um die Meldung zu schließen. Das Makro wird dann nicht überschrieben.



Erstellen eines Tastaturmakros

So erstellen Sie ein Makro:

1. Klicken Sie auf "Keyboard" > "Keyboard Macros" (Tastatur > Tastaturmakros). Das Dialogfeld "Keyboard Macros" (Tastaturmakros) wird angezeigt.
2. Klicken Sie auf "Add" (Hinzufügen). Das Dialogfeld "Add Keyboard Macro" (Tastaturmakro hinzufügen) wird angezeigt.
3. Geben Sie im Feld "Keyboard Macro Name" (Name des Tastaturmakros) einen Namen für das Makro ein. Dieser Name wird nach der Erstellung im Tastaturmenü angezeigt.
4. Wählen Sie in der Dropdownliste im Feld "Hot-Key Combination" (Zugriffstastenkombination) eine Tastenkombination aus. Dies ermöglicht es Ihnen, das Makro mit einer vordefinierten Tastenkombination auszuführen. ***///Optional***
5. Wählen Sie in der Dropdownliste "Keys to Press" (Zu betätigende Tasten) alle Tasten aus, die Sie verwenden möchten, um die Tastenkombination zu emulieren, die zum Ausführen des Befehls verwendet wird. Wählen Sie die Tasten in der Reihenfolge aus, in der sie betätigt werden sollen. Wählen Sie nach jeder gewählten Taste "Add Key" (Taste hinzufügen) aus. Nach der Auswahl jeder Taste wird diese im Feld "Macro Sequence" (Makrosequenz) angezeigt und ein Befehl zum Freigeben der Taste wird automatisch hinzugefügt.



6. Um die Funktion "Send Text to Target" (Text an Ziel senden) für das Makro zu verwenden, klicken Sie auf die Schaltfläche "Construct Macro from Text" (Makro aus Text erstellen).
7. Erstellen Sie beispielsweise ein Makro zum Schließen eines Fensters durch die Tastenkombination "Linke Strg-Taste+Esc". Dieses wird im Feld "Macro Sequenz" (Makrosequenz) wie folgt angezeigt:

   Linke Strg-Taste drücken

   Linke Strg-Taste freigeben

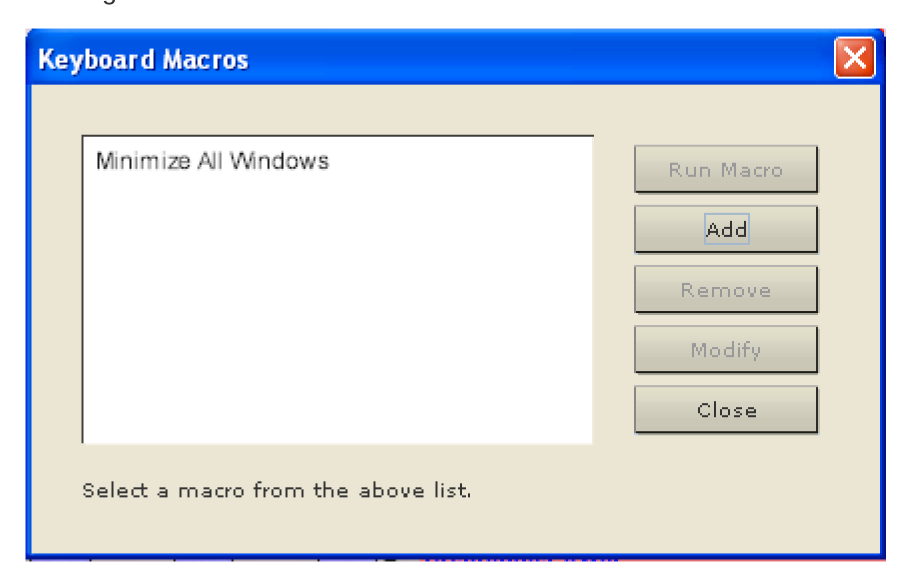
   Esc drücken

   Esc freigeben

8. Überprüfen Sie das Feld "Macro Sequence" (Makrosequenz), um sicherzustellen, dass die Makrosequenz korrekt definiert wurde.
   a. Wenn Sie einen Schritt aus der Sequenz entfernen möchten, markieren Sie diesen, und klicken Sie auf "Remove" (Entfernen).
   b. Wenn Sie die Reihenfolge der Schritte in der Sequenz ändern möchten, klicken Sie auf den Schritt und anschließend auf die Pfeil-nach-oben- oder Pfeil-nach-unten-Taste, um die Position des Schritts wie gewünscht zu ändern.
9. Klicken Sie zum Speichern des Makros auf "OK". Klicken Sie auf "Clear" (Löschen), um alle Felder zu löschen und erneut mit der Auswahl zu beginnen. Wenn Sie auf "OK" klicken, wird das Dialogfenster "Keyboard Macros" (Tastaturmakros) mit dem neuen Tastaturmakro angezeigt.



10. Klicken Sie im Dialogfeld "Keyboard Macros" (Tastaturmakros) auf "Close" (Schließen). Das Makro wird nun im Tastaturmenü der Anwendung angezeigt. Wählen Sie das neue Makro im Menü aus, um es auszuführen, oder verwenden Sie die dem Makro zugeordnete Tastenkombination.



Ausführen eines Tastaturmakros

Wenn Sie ein Tastaturmakro erstellt haben, können Sie es über das zugeordnete Tastaturmakro ausführen oder es aus dem Tastaturmenü auswählen.

Ausführen eines Makros über die Menüleiste

Ein erstelltes Makro wird im Menü "Keyboard" (Tastatur) angezeigt. Führen Sie das Tastaturmakro aus, indem Sie im Menü "Keyboard" (Tastatur) auf das Makro klicken.

Ausführen eines Makros mithilfe einer Tastaturkombination

Wenn Sie beim Erstellen eines Makros eine Tastenkombination zugewiesen haben, können Sie das Makro durch Drücken der entsprechenden Tasten ausführen. Drücken Sie beispielsweise gleichzeitig die Tasten Strg+Alt+0, um alle Fenster auf einem Windows-Zielserver zu minimieren.

Bearbeiten und Löschen von Tastaturmakros

► **So ändern Sie ein Makro:**

1. Wählen Sie **Keyboard > Keyboard Macros** (Tastatur > Tastaturmakros). Das Dialogfeld "Keyboard Macros" (Tastaturmakros) wird angezeigt.
2. Wählen Sie das gewünschte Makro aus der Liste aus.

3. Klicken Sie auf **Modify** (Ändern). Das Dialogfeld **Add/Edit Macro** (Makro hinzufügen/bearbeiten) wird angezeigt.
4. Nehmen Sie die gewünschten Änderungen vor.
5. Klicken Sie auf OK.

So entfernen Sie ein Makro:

1. Wählen Sie **Keyboard > Keyboard Macros** (Tastatur > Tastaturmakros). Das Dialogfeld "Keyboard Macros" (Tastaturmakros) wird angezeigt.
2. Wählen Sie das gewünschte Makro aus der Liste aus.
3. Klicken Sie auf "Remove" (Entfernen). Das Makro wird gelöscht.

STRG+ALT+ENTF-Makro

Aufgrund der häufigen Verwendung dieser Tastenkombination ist ein Makro STRG+ALT+ENTF vorprogrammiert. Wenn Sie auf der Symbolleiste auf die Verknüpfung Ctrl+Alt+Delete (STRG+ALT+ENTF) DEL klicken, wird diese Tastenfolge an den Server oder KVM-Switch gesendet, mit dem Sie zurzeit verbunden sind.

Wenn Sie aber bei der Verwendung des MPC oder RRC die Tastenkombination STRG+ALT+ENTF drücken, wird diese Eingabe aufgrund der Struktur des Windows-Betriebssystems zunächst von Ihrem eigenen PC interpretiert, anstatt die Tastenfolge wie gewünscht an den Zielserver zu senden.

Einstellungen für CIM-Tastatur/Mausoptionen

So greifen Sie auf das DCIM-USBG2-Setupmenü zu:

1. Klicken Sie mit der Maus in ein Fenster, wie z. B. Windows-Editor (Windows®-Betriebssystem) o. Ä.
2. Wählen Sie die Optionen für "Set CIM Keyboard/Mouse options" (CIM-Tastatur/-Maus festlegen) aus. Dies ist das Äquivalent für das Senden von linke Strg-Taste und Num Lock an das Ziel. Die Optionen für das CIM-Setupmenü werden angezeigt.
3. Legen Sie die Sprache und Mauseinstellungen fest.
4. Verlassen Sie das Menü, um zur normalen CIM-Funktionalität zurückzukehren.



Videoeigenschaften

Aktualisieren der Anzeige

Der Befehl "Refresh Screen" (Anzeige aktualisieren) erzwingt eine Aktualisierung des Videobildschirms. Videoeinstellungen können auf verschiedene Art und Weise automatisch aktualisiert werden:

- Der Befehl "Refresh Screen" (Anzeige aktualisieren) erzwingt eine Aktualisierung des Videobildschirms.
- Mit dem Befehl "Auto-sense Video Settings" (Videoeinstellungen automatisch erkennen) werden die Videoeinstellungen des Zielservers automatisch erkannt.
- Mit dem Befehl "Calibrate Color" (Farbe kalibrieren) wird das Videobild kalibriert, um die angezeigten Farben zu verbessern.

Darüber hinaus können Sie die Einstellungen manuell über den Befehl "Video Settings" (Videoeinstellungen) anpassen.

Führen Sie einen der folgenden Schritte aus, um die Videoeinstellungen zu aktualisieren:

- Wählen Sie "Video" > "Refresh Screen" (Video > Anzeige aktualisieren) aus oder klicken Sie auf die Schaltfläche "Refresh Screen" (Anzeige aktualisieren) in der Symbolleiste.

Auto-Sense Video Settings (Videoeinstellungen automatisch erkennen)

Der Befehl "Auto-sense Video Settings" (Videoeinstellungen automatisch erkennen) erzwingt das erneute Erkennen der Videoeinstellungen (Auflösung, Aktualisierungsfrequenz) und erstellt die Videoanzeige neu.

Führen Sie zur automatischen Erkennung der Videoeinstellungen die folgenden Schritte aus:

- Wählen Sie "Video" > "Auto-sense Video Settings" (Video > Videoeinstellungen automatisch erkennen) aus oder klicken Sie auf die Schaltfläche "Auto-Sense Video Settings" (Videoeinstellungen automatisch erkennen) in der Symbolleiste. Eine Meldung mit der Information, dass die automatische Anpassung läuft, wird angezeigt.



Kalibrieren der Farben

Verwenden Sie den Befehl "Calibrate Color" (Farbe kalibrieren), um die Farbstufen (Farbton, Helligkeit, Sättigung) der übertragenen Videobilder zu optimieren. Die Farbeinstellungen basieren auf dem jeweiligen Zielserver.

Hinweis: Der Befehl "Calibrate Color" (Farbe kalibrieren) gilt nur für die aktuelle Verbindung.

Hinweis: Das Modell KX II-101 unterstützt die Kalibrierung der Farben.

Um die Farbe zu kalibrieren, führen Sie Folgendes durch:

- Wählen Sie "Video" > "Calibrate Color" (Video > Farbe kalibrieren) oder klicken Sie auf die Schaltfläche "Calibrate Color" (Farbe kalibrieren) in der Symbolleiste. Die Farbkalibrierung des Zielgerätebildschirms wird aktualisiert.

Konfigurieren von Videoeinstellungen

Verwenden Sie den Befehl "Video Settings" (Videoeinstellungen), um die Videoeinstellungen manuell anzupassen.

So ändern Sie die Videoeinstellungen:

1. Wählen Sie "Video" > "Video Settings" (Video > Videoeinstellungen) aus oder klicken Sie auf die Schaltfläche "Video Settings" (Videoeinstellungen) in der Symbolleiste, um das Dialogfeld "Video Settings" (Videoeinstellungen) zu öffnen.
2. Passen Sie die folgenden Einstellungen nach Wunsch an. Wenn Sie die Einstellungen anpassen, sind die Änderungen sofort sichtbar:
   a. Noise Filter (Rauschfilter)

      Das Gerät kann elektrische Störungen aus der Videoausgabe von Grafikkarten herausfiltern. Dieses Feature optimiert die Bildqualität und reduziert die Bandbreite. Höhere Einstellungen übermitteln nur dann Variantenpixel, wenn bei einem Vergleich mit den Nachbarpixeln eine starke Farbabweichung vorliegt. Eine zu hohe Einstellung des Grenzwerts kann jedoch zu einer unbeabsichtigten Filterung von gewünschten Bildschirmänderungen führen.
      Niedrigere Einstellungen übermitteln die meisten Pixeländerungen. Eine zu niedrige Einstellung dieses Grenzwerts kann zu einer höheren Bandbreitenverwendung führen.

   b. PLL Settings (PLL-Einstellungen)



Clock (Uhr) – Diese Option steuert, wie schnell Videopixel auf dem Videobildschirm angezeigt werden. Änderungen an den Uhreinstellungen führen zu einer horizontalen Streckung oder Stauchung des Videobilds. Als Einstellung werden ungerade Zahlen empfohlen. Üblicherweise sollte diese Einstellung nicht geändert werden, da die automatische Erkennung meist korrekt ist.

Phase – Die Phasenwerte liegen zwischen 0 und 31 und werden zyklisch durchlaufen. Halten Sie bei dem Phasenwert an, der das beste Videobild für den aktiven Zielserver ergibt.

c. Brightness (Helligkeit): Mithilfe dieser Einstellung passen Sie die Helligkeit der Zielserveranzeige an.

d. Brightness Red (Helligkeit – Rot) – Steuert die Helligkeit der Anzeige des Zielservers für das rote Signal.

e. Brightness Green (Helligkeit – Grün) – Steuert die Helligkeit des grünen Signals.

f. Brightness Blue (Helligkeit – Blau) – Steuert die Helligkeit des blauen Signals.

g. Contrast Red (Kontrast – Rot) – Steuert den Kontrast des roten Signals.

h. Contrast Green (Kontrast – Grün) – Steuert das grüne Signal.

i. Contrast Blue (Kontrast – Blau) – Steuert das blaue Signal.

Wenn das Videobild extrem verschwommen oder unscharf wirkt, können die Einstellungen für die Uhr und die Phase so gewählt werden, dass auf dem aktiven Zielserver ein besseres Bild angezeigt wird.

Warnung: Gehen Sie beim Ändern der Einstellungen für die Uhr und die Phase sorgfältig vor. Änderungen können zu Verzerrungen oder sogar zum Verlust des Videobildes führen, und Sie können möglicherweise die vorherigen Einstellungen nicht wiederherstellen. Wenden Sie sich an den technischen Kundendienst von Raritan, bevor Sie Änderungen vornehmen.

---

j. Horizontal Offset (Horizontaloffset) – Steuert die horizontale Positionierung der Zielserveranzeige auf dem Bildschirm.

k. Vertical Offset (Vertikaloffset) – Steuert die vertikale Positionierung der Zielserveranzeige auf dem Bildschirm.

3. Wählen Sie "Automatic Color Calibration" (Automatische Farbkalibrierung) aus, um diese Funktion zu aktivieren.
4. Wählen Sie den Videoerkennungsmodus aus:



- Best possible video mode (Bestmöglicher Videomodus)

  Beim Wechseln von Zielgeräten oder Zielauflösungen führt das Gerät die vollständige automatische Erkennung durch. Bei dieser Option wird das Videobild so kalibriert, dass die bestmögliche Bildqualität erzielt wird.

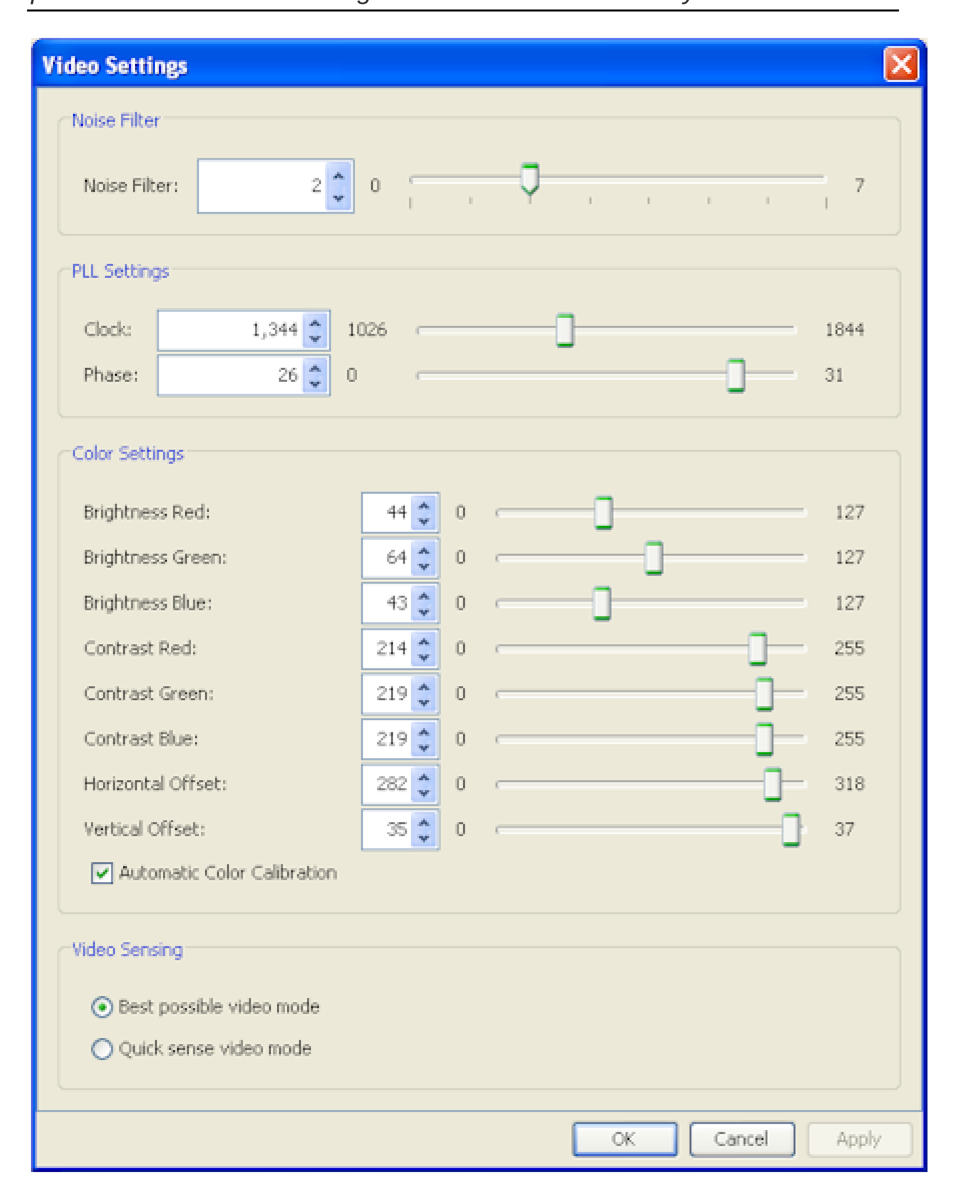
- Quick sense video mode (Videomodus schnell erkennen)

  Bei dieser Option führt das Gerät eine schnelle automatische Erkennung des Videomodus durch, um das Bild des Zielgeräts schneller anzuzeigen. Diese Option eignet sich insbesondere für die Eingabe der BIOS-Konfiguration eines Zielservers nach einem Neustart.

5. Klicken Sie auf OK, um die Einstellungen zu übernehmen, und schließen Sie das Dialogfenster. Klicken Sie auf "Apply" (Übernehmen), um die Einstellungen zu übernehmen, ohne das Dialogfenster zu schließen.



Hinweis: Einige Sun-Hintergrundanzeigen (z. B. Anzeigen mit sehr dunklen Rändern) werden auf bestimmten Sun-Servern nicht exakt zentriert abgebildet. Verwenden Sie einen anderen Hintergrund, oder platzieren Sie auf der Anzeige oben links ein helleres Symbol.





Verwenden der Funktion "Screenshot from Target" (Screenshot vom Zielgerät)

Mit dem Befehl "Screenshot from Target" (Screenshot vom Zielgerät) können Sie einen Screenshot vom Zielserver aufnehmen. Speichern Sie diesen Screenshot ggf. an einem Speicherort Ihrer Wahl als Bitmap-, JPEG- oder PNG-Datei ab.

▸ So nehmen Sie einen Screenshot vom Zielserver auf:

1. Wählen Sie "Video" > "Screenshot from Target" (Video > Screenshot vom Zielgerät) aus oder klicken Sie auf die Schaltfläche "Screenshot from Target" (Screenshot vom Zielgerät) in der Symbolleiste.
2. Wählen Sie im Dialogfenster "Save" (Speichern) den Speicherort für die Datei aus, benennen Sie sie und wählen Sie ein Dateiformat aus der Dropdownliste "Files of Type" (Dateitypen) aus.
3. Klicken Sie zum Speichern des Screenshots auf "Save" (Speichern).





Ändern der höchsten Aktualisierungsrate

Wenn die von Ihnen verwendete Videokarte kundenspezifische Software verwendet und Sie über MPC oder VKC auf das Ziel zugreifen, kann es erforderlich sein, die maximale Aktualisierungsrate des Monitors zu ändern, damit die Aktualisierungsrate für das Ziel wirksam wird.

▶ So stellen Sie die Aktualisierungsrate des Monitors ein:

1. Wählen Sie unter Windows® "Eigenschaften von Anzeige" > "Einstellungen" > "Erweitert" aus, um das Dialogfeld "Eigenschaften von Plug-and-Play-Monitor" zu öffnen.
2. Klicken Sie auf die Registerkarte "Monitor".
3. Legen Sie die "Screen Refresh Rate" (Bildschirmaktualisierungsrate) fest.
4. Klicken Sie auf "OK" und anschließend erneut auf "OK", um die Einstellungen zu übernehmen.

Mausoptionen

Bei der Steuerung eines Zielservers zeigt die Remotekonsole zwei Cursor an: Ein Cursor gehört zur Client-Workstation und der andere zum Zielserver.

Sie können entweder im Ein-Cursor-Modus oder im Zwei-Cursor-Modus arbeiten. Wenn Sie sich im Zwei-Cursor-Modus befinden und die Option ordnungsgemäß konfiguriert wurde, werden die Cursor aneinander ausgerichtet.

Bei zwei Cursorn bietet das Gerät verschiedene Mausmodi:

- "Absolute" (Absolute Mouse Synchronization)
- "Intelligent" (Intelligenter Mausmodus)
- "Standard" (Standardmausmodus)

Mauszeigersynchronisation

Bei der Remoteanzeige eines Zielservers mit einer Maus werden zwei Cursor angezeigt: Ein Mauszeiger gehört zur Remote-Client-Workstation und der andere zum Zielserver. Wenn sich der Mauszeiger im Zielserverfenster des Virtual KVM Client befindet, werden Mausbewegungen und Klicks direkt an den angeschlossenen Zielserver übermittelt. Aufgrund der Mausbeschleunigungseinstellungen sind die Bewegungen des Client-Mauszeigers etwas schneller als die des Zielgerätmauszeigers.

Bei schnellen LAN-Verbindungen können Sie den Mauszeiger des Virtual KVM Client deaktivieren, um nur den Cursor des Zielservers anzuzeigen. Sie können zwischen den beiden Modi (ein Cursor und zwei Cursor) wechseln.

Tipps zur Maussynchronisation

Führen Sie bei der Konfiguration der Maussynchronisierung folgende Schritte aus:

1. Stellen Sie sicher, dass die ausgewählte Videoauflösung und die Aktualisierungsfrequenz vom Gerät unterstützt werden. Im Dialogfeld "Virtual KVM Client Connection Info" (Virtual KVM Client – Verbindungsinformationen) werden die tatsächlich vom Gerät erkannten Werte angezeigt.
2. Stellen Sie sicher, dass die Kabellänge bei KX II- und LX-Geräten die Grenzwerte für die ausgewählte Videoauflösung nicht überschreitet.
3. Stellen Sie sicher, dass Maus und Monitor während der Installation richtig konfiguriert wurden.
4. Führen Sie eine automatische Erkennung durch, indem Sie im Virtual KVM Client auf die Schaltfläche "Auto-sense Video" (Video automatisch erkennen) klicken.
5. Führen Sie folgende Schritte aus, falls dadurch die Maussynchronisation (bei Linux-, UNIX- und Solaris-KVM-Zielservern) nicht verbessert wird:
   a. Öffnen Sie ein Terminalfenster.
   b. Geben Sie den Befehl `xset mouse 1 1` ein.
   c. Schließen Sie das Terminalfenster.
6. Klicken Sie im Virtual KVM Client auf die Schaltfläche zur Maussynchronisierung .



Weitere Hinweise zum Mausmodus "Intelligent"

- Stellen Sie sicher, dass sich links oben auf dem Bildschirm keine Symbole oder Anwendungen befinden, da in diesem Bereich die Synchronisierungsroutine ausgeführt wird.
- Verwenden Sie keinen animierten Cursor.
- Deaktivieren Sie den Active Desktop auf KVM-Zielservern.

Synchronize Mouse (Maus synchronisieren)

Im Zwei-Cursor-Modus erzwingt der Befehl "Synchronize Mouse" (Maus synchronisieren) die erneute Ausrichtung des Zielserver-Mauszeigers am Mauszeiger des Virtual KVM Client.

Führen Sie einen der folgenden Schritte aus, um die Maus zu synchronisieren:

- Wählen Sie "Mouse" > "Synchronize Mouse" (Maus > Maus synchronisieren) aus oder klicken Sie auf die Schaltfläche "Synchronize Mouse" (Maus synchronisieren) in der Symbolleiste.

Hinweis: Diese Option steht nur in den Mausmodi "Standard" und "Intelligent" zur Verfügung.

Mausmodus "Standard"

Beim Mausmodus "Standard" wird ein Standard-Maussynchronisierungsalgorithmus mit relativen Mauspositionen verwendet. Für den Mausmodus "Standard" müssen die Mausbeschleunigung deaktiviert und andere Mausparameter korrekt eingerichtet werden, damit die Client- und die Servermaus synchron bleiben.

So gelangen Sie in den Mausmodus "Standard":

- Wählen Sie **Mouse > Standard** (Maus > Standard).

Intelligenter Mausmodus

Im Mausmodus "Intelligent" erkennt das Gerät die Mauseinstellungen des Zielgeräts und kann die Cursor dementsprechend synchronisieren, wodurch die Mausbeschleunigung auf dem Zielgerät ermöglicht wird. Intelligenter Mausmodus wird standardmäßig für nicht-VM-Ziele verwendet.

Bei der Synchronisierung "tanzt" der Cursor in der oberen linken Ecke des Bildschirms und berechnet die Beschleunigung. Damit dieser Modus richtig funktioniert, müssen bestimmte Bedingungen erfüllt sein.

So gelangen Sie in den intelligenten Mausmodus:

- Wählen Sie "Mouse > Intelligent" (Maus > Intelligent).

Bedingungen für die intelligente Maussynchronisation

Der Befehl "Intelligent Mouse Synchronization" (Intelligente Maussynchronisierung) im Menü "Mouse" (Maus) synchronisiert automatisch die Cursor in Inaktivitätsphasen. Zur korrekten Synchronisierung müssen jedoch folgende Bedingungen erfüllt sein:

- Der Active Desktop muss auf dem Zielgerät deaktiviert sein.
- Oben in der linken Ecke auf der Zielseite dürfen keine Fenster angezeigt werden.
- Oben in der linken Ecke auf der Zielseite darf kein animierter Hintergrund vorhanden sein.
- Der Zielcursor muss standardmäßig und nicht animiert sein.
- Die Geschwindigkeit des Zielcursors darf nicht auf sehr hohe oder sehr niedrige Werte eingestellt sein.
- Erweiterte Mauseigenschaften wie "Enhanced pointer precision" (Zeigerbeschleunigung verbessern) oder "Snap mouse to default button in dialogs" (In Dialogfeldern automatisch zur Standardschaltfläche springen) müssen deaktiviert sein.
- Wählen Sie im Fenster "Video Settings" (Videoeinstellungen) die Option "Best Possible Video Mode" (Bestmöglicher Videomodus) aus.
- Die Ränder des Zielvideos müssen deutlich sichtbar sein. Ein schwarzer Rand muss also bei einem Bildlauf zu einem Rand des Zielvideobilds zwischen dem Zieldesktop und dem Fenster der KVM-Remotekonsole sichtbar sein.
- Wenn Sie die Funktion zur intelligenten Maussynchronisierung nutzen, können Datei- oder Ordnersymbole in der linken oberen Ecke Ihres Desktops zu Problemen führen. Um Probleme mit dieser Funktion zu vermeiden, empfiehlt Raritan, Datei- oder Ordnersymbole in der linken oberen Ecke Ihres Desktops zu entfernen.



Initiieren Sie nach dem automatischen Erkennen des Zielvideos manuell eine Maussynchronisierung. Klicken Sie dazu in der Symbolleiste auf die Schaltfläche "Synchronize Mouse" (Maus synchronisieren). Dies gilt auch bei Änderung der Auflösung des Zielgeräts, wenn die Cursor nicht mehr synchronisiert sind.

Schlägt die intelligente Maussynchronisierung fehl, wird die Standardeinstellung der Maussynchronisierung wiederhergestellt.

Beachten Sie, dass die Mauskonfigurationen auf unterschiedlichen Zielbetriebssystemen variieren. Weitere Informationen finden Sie in den Richtlinien für Ihr Betriebssystem. Die intelligente Maussynchronisierung ist für UNIX-Zielgeräte nicht verfügbar.

Mausmodus "Absolut"

In diesem Modus werden absolute Koordinaten verwendet, um die Cursor von Client und Zielgerät synchron zu halten, auch wenn für die Maus des Zielgeräts eine andere Beschleunigung oder Geschwindigkeit eingestellt wurde. Dieser Modus wird von Servern mit USB-Ports unterstützt und ist der Standardmodus für VM- und duale VM-Ziele.

So gelangen Sie in den Mausmodus „Absolute“ (Absolut):

- Wählen Sie **Mouse > Absolute** (Maus > Absolut).

Hinweis: Der Mausmodus "Absolute Mouse Synchronization" (Absolute Maussynchronisierung) steht für LX nur für USB-CIMs (D2CIM-VUSB und D2CIM-DVUSB) mit Aktivierung für virtuelle Medien zur Verfügung.

Ein-Cursor-Modus

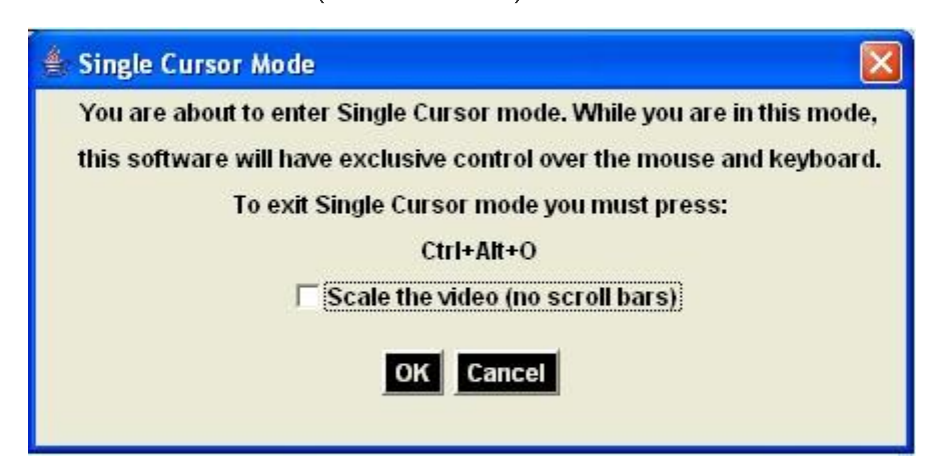
Beim Ein-Cursor-Modus wird nur der Cursor des Zielservers verwendet; der lokale Mauszeiger wird nicht mehr angezeigt. Im Ein-Cursor-Modus steht der Befehl "Synchronize Mouse" (Maus synchronisieren) nicht zur Verfügung, da ein einzelner Mauszeiger nicht synchronisiert werden muss.

Hinweis: Der Ein-Cursor-Modus funktioniert nicht auf Windows- oder Linux-Zielgeräten, wenn VM als Client verwendet wird.

Führen Sie folgende Schritte aus, um den Ein-Cursor-Modus zu aktivieren:

1. Wählen Sie **Mouse > Single Mouse Cursor** (Maus > Ein Cursor).

2. Klicken Sie in der Symbolleiste auf die Schaltfläche "Single/Double Mouse Cursor" (Ein/Zwei Cursor).



▶ **So beenden Sie den Ein-Cursor-Modus:**

- Drücken Sie **Strg+Alt+O** auf der Tastatur, um den Ein-Cursor-Modus zu beenden.

Optionen im Menü "Tools" (Extras)

"General Settings" (Allgemeine Einstellungen)

▶ **So legen Sie die Optionen im Menü "Tools" (Extras) fest:**

1. Wählen Sie "Tools" (Extras) > "Options" (Optionen). Das Dialogfeld "Options" (Optionen) wird angezeigt.
2. Aktivieren Sie das Kontrollkästchen "Enable Logging" (Protokollierung aktivieren) nur nach Anweisung durch den technischen Kundendienst. Bei dieser Option wird im Basisverzeichnis eine Protokolldatei erstellt.
3. Wählen Sie ggf. in der Dropdown-Liste "Keyboard Type" (Tastaturtyp) einen Tastaturtyp aus. Folgende Optionen stehen zur Verfügung:
   - US/International (USA/International)
   - French (France) (Französisch)
   - German (Germany) (Deutsch)
   - Japanese (Japanisch)
   - United Kingdom (Großbritannien)
   - Korean (Korea) (Koreanisch)
   - French (Belgium) (Französisch, Belgien)



- Norwegian (Norway) (Norwegisch)
- Portugiesisch (Portugal)
- Danish (Denmark) (Dänisch)
- Swedish (Sweden) (Schwedisch)
- German (Deutsch, Schweiz)
- Hungarian (Hungary) (Ungarisch)
- Spanish (Spain) (Spanisch)
- Italian (Italy) (Italienisch)
- Slovenian (Slowenisch)
- Übersetzung: Französisch – Englisch (USA)
- Übersetzung: Französisch – Englisch (USA/International)

Beim AKC entspricht der Tastaturtyp standardmäßig dem lokalen Client. In diesem Fall trifft die Option nicht zu. Darüber hinaus unterstützen die Modelle KX II-101 und KX II-101-V2 den Ein-Cursor-Modus nicht. Daher ist die Funktion "Exit Single Cursor Mode" (Ein-Cursor-Modus beenden) für diese Geräte nicht verfügbar.

4. Konfigurieren von Zugriffstasten:
   - "Exit Full Screen Mode - Hotkey" (Zugriffstaste zum Beenden des Vollbildmodus). Wenn Sie in den Vollbildmodus wechseln, erscheint die Anzeige des Zielservers im Vollbildmodus mit derselben Auflösung wie auf dem Zielserver. Diese Zugriffstaste wird zum Beenden des Modus verwendet.
   - "Exit Single Cursor Mode - Hotkey" (Zugriffstaste zum Beenden des Ein-Cursor-Modus). Im Ein-Cursor-Modus wird nur der Cursor des Zielservers angezeigt. Diese Zugriffstaste wird zum Beenden des Ein-Cursor-Modus verwendet, sodass der Client-Cursor wieder angezeigt wird.
   - "Disconnect from Target - Hotkey" (Zugriffstaste zum Trennen der Verbindung mit dem Ziel): Aktivieren Sie diese Zugriffstaste, damit Benutzer die Verbindung mit dem Ziel unverzüglich trennen können.

   Bei der Kombination mehrerer Zugriffstasten kann eine Tastenkombination jeweils nur einer Funktion zugewiesen werden. Wenn die Taste "Q" beispielsweise bereits der Funktion "Disconnect from Target" (Verbindung mit dem Ziel trennen) zugewiesen ist, ist sie für die Funktion "Exit Full Screen Mode" (Vollbildmodus beenden) nicht mehr verfügbar. Wenn eine Zugriffstaste bei einer Aktualisierung hinzugefügt wird und der Standardwert für die Taste bereits verwendet wird, wird der Funktion stattdessen der nächste verfügbare Wert zugewiesen.

5. Klicken Sie auf "OK".

Tastaturbeschränkungen

Türkische Tastaturen

Bei Verwendung einer türkischen Tastatur müssen Sie die Verbindung mit einem Zielserver über den Active KVM Client (AKC) herstellen. Von anderen Raritan-Clients wird es nicht unterstützt.

Slowenische Tastaturen

Aufgrund einer JRE-Beschränkung funktioniert die Taste < auf slowenischen Tastaturen nicht.

Sprachkonfiguration für Linux

Da mit der Sun-JRE auf einem Linux-Betriebssystem Probleme bei der korrekten Erzeugung von KeyEvents (Tastenereignissen) für fremdsprachige Tastaturen auftreten, die mithilfe der Systemeinstellungen konfiguriert wurden, empfiehlt Raritan die Konfiguration fremdsprachiger Tastaturen mithilfe der in der folgenden Tabelle beschriebenen Methoden.

Sprache	Konfigurationsmethode
USA/Int.	Standard
Französisch	Keyboard Indicator (Tastaturanzeige)
Deutsch (Deutschland)	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]
Japanisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]
Britisches Englisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]
Koreanisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]
Belgisch	Keyboard Indicator (Tastaturanzeige)
Norwegisch	Keyboard Indicator (Tastaturanzeige)
Dänisch	Keyboard Indicator (Tastaturanzeige)
Schwedisch	Keyboard Indicator (Tastaturanzeige)
Ungarisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]
Spanisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]
Italienisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]
Slowenisch	System Settings (Control Center)



Sprache	Konfigurationsmethode
	[Systemeinstellungen (Steuerzentrale)]
Portugiesisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]

Hinweis: Die Tastaturanzeige sollte bei Linux-Systemen, die Gnome als Desktopumgebung nutzen, verwendet werden.

"Client Launch Settings" (Client-Starteinstellungen)

LX-Benutzer können die Starteinstellungen für den Client konfigurieren, um die Einstellungen des Bildschirms für eine KVM-Sitzung zu definieren.

Hinweis: Diese Funktion ist im MPC, jedoch nicht im AKC oder VKC verfügbar.

So konfigurieren Sie Starteinstellungen für den Client:

1. Wählen Sie "Tools" (Extras) > "Options" (Optionen). Das Dialogfeld "Options" (Optionen) wird angezeigt.
2. Klicken Sie auf die Registerkarte "Client Launch Settings" (Client-Starteinstellungen).
   - So konfigurieren Sie die Zielfenstereinstellungen:

   a. Wählen Sie "Standard - sized to target Resolution" (Standard - Größe an Zielauflösung anpassen) aus, um das Fenster mit der aktuellen Auflösung des Ziels zu öffnen. Wenn die Zielauflösung größer als die Client-Auflösung ist, bedeckt das Zielfenster soviel Bildschirmfläche wie möglich. Gegebenenfalls werden Bildlaufleisten hinzugefügt.

   b. Wählen Sie "Full Screen" (Vollbild) aus, um das Zielfenster im Vollbildmodus zu öffnen.

   - So konfigurieren Sie den Monitor, auf dem der Ziel-Viewer gestartet wird:

   a. Wählen Sie "Monitor Client Was Launched from" (Monitor-Client gestartet von) aus, wenn der Ziel-Viewer in derselben Anzeige wie die auf dem Client verwendete Anwendung gestartet werden soll (z. B. ein Webbrowser oder ein Applet).

   b. Wählen Sie "Select From Detected Monitors" (Aus gefundenen Monitoren auswählen) aus, um einen Monitor aus einer Liste mit Monitoren auszuwählen, die von der Anwendung gefunden wurden. Wenn ein zuvor ausgewählter Monitor nicht mehr gefunden wird, wird "Currently Selected Monitor Not Detected" (Aktuell ausgewählter Monitor nicht gefunden) angezeigt.

   - So konfigurieren Sie zusätzliche Starteinstellungen:

a. Wählen Sie "Enable Single Cursor Mode" (Ein-Cursor-Modus aktivieren), um den Ein-Cursor-Modus bei Zugriff auf den Server als Standardmausmodus zu aktivieren.

b. Wählen Sie "Enable Scale Video" ("Video skalieren" aktivieren) aus, damit die Anzeige auf dem Zielserver automatisch skaliert wird, sobald auf ihn zugegriffen wird.

c. Wählen Sie "Pin Menu Toolbar" (Menüsymbolleiste anheften), wenn die Symbolleiste auf dem Ziel im Vollbildmodus sichtbar bleiben soll. Wenn sich das Ziel im Vollbildmodus befindet, ist das Menü in der Standardeinstellung nur sichtbar, wenn Sie mit der Maus auf den oberen Bildschirmrand zeigen.

3. Klicken Sie auf "OK".

"Scan Settings" (Scaneinstellungen)

LX ermöglicht eine Port-Scanfunktion, mit der nach ausgewählten Zielen gesucht werden kann. Die Ziele werden dann in einer Bildschirmpräsentationsansicht angezeigt. So können Sie bis zu 32 Ziele gleichzeitig überwachen. Sie können je nach Bedarf eine Verbindung mit mehreren Zielen herstellen oder sich auf ein bestimmtes Ziel konzentrieren. Scanvorgänge können Standardserver, Dominion-Schichtgeräte und KVM-Switch-Ports umfassen. Siehe ***Scannen von Ports*** (auf Seite 51). Das Scanintervall und die Standardanzeigeoptionen legen Sie auf der Registerkarte "Scan Settings" (Scaneinstellungen) fest.

► **So legen Sie die Scaneinstellungen fest:**

1. Wählen Sie "Tools" (Extras) > "Options" (Optionen). Das Dialogfeld "Options" (Optionen) wird angezeigt.
2. Wählen Sie die Registerkarte "Scan Settings" (Scaneinstellungen) aus.
3. Geben Sie im Feld "Display Interval (10-255 sec):" (Anzeigeintervall (10-255 Sek.)) die Anzahl Sekunden ein, die das Ziel im Fokus in der Mitte des Fensters "Port Scan" (Port-Scan) angezeigt werden soll.
4. Geben Sie im Feld "Interval Between Ports (10 - 255 sec):" (Intervall zwischen Ports (10-255 Sek.)) das Intervall ein, in dem das Gerät zwischen Ports pausieren soll.
5. Ändern Sie im Abschnitt "Display" (Anzeige) die Standardanzeigeoptionen für die Größe der Miniaturansichten und die Teilung der Ausrichtung des Fensters "Port Scan" (Port-Scan).
6. Klicken Sie auf "OK".



Ansichtsoptionen

View Toolbar (Symbolleiste anzeigen)

Sie können den Virtual KVM Client mit oder ohne die Symbolleiste verwenden.

So blenden Sie die Symbolleiste ein bzw. aus:

- Wählen Sie **View > View Toolbar** (Ansicht > Symbolleiste anzeigen).

"View Status Bar" (Statusleiste anzeigen)

Standardmäßig wird die Statusleiste unten im Zielfenster angezeigt.

So blenden Sie die Statusleiste aus:

- Klicken Sie auf "View" (Ansicht) > "Status Bar" (Statusleiste), um die Option zu deaktivieren.

So stellen Sie die Statusleiste wieder her:

- Klicken Sie auf "View" (Ansicht) > "Status Bar" (Statusleiste), um die Option zu aktivieren.

Scaling (Skalieren)

Das Skalieren des Zielfensters ermöglicht die Anzeige des gesamten Inhalts des Zielserverfensters. Dieses Feature vergrößert oder verkleinert das Zielvideobild unter Beibehaltung des Seitenverhältnisses, um es an die Fenstergröße des Virtual KVM Client anzupassen. Somit wird der gesamte Zielserverdesktop angezeigt, und Sie müssen nicht die Bildlaufleiste verwenden.

So aktivieren bzw. deaktivieren Sie die Skalierung:

- Wählen Sie **View > Scaling** (Ansicht > Skalieren).

Vollbildmodus

Wenn Sie in den Vollbildmodus wechseln, erscheint die Anzeige des Zielservers im Vollbildmodus mit derselben Auflösung wie auf dem Zielserver. Die Zugriffstaste, über die Sie diesen Modus beenden können, legen Sie im Dialogfeld "Options" (Optionen) fest (siehe ***"Tool Options" (Tool-Optionen)*** (siehe "***Optionen im Menü "Tools" (Extras)***" auf Seite 86)).

Wenn Sie im Vollbildmodus den Mauszeiger an den oberen Bildschirmrand schieben, wird die Menüleiste für den Vollbildschirmmodus angezeigt. Wenn die Menüleiste im Vollbildmodus sichtbar bleiben soll, aktivieren Sie die Option "Pin Menu Toolbar" (Menüsymbolleiste anheften) im Dialogfeld "Tool Options" (Tool-Optionen). Siehe ***"Tool Options" (Tool-Optionen)*** (siehe "***Optionen im Menü "Tools" (Extras)***" auf Seite 86).

So gelangen Sie in den Vollbildmodus:

- Wählen Sie "View" > "Full Screen" (Ansicht > Vollbild) aus.

So beenden Sie den Vollbildmodus:

- Drücken Sie die im Dialogfeld "Options" (Optionen) konfigurierte Zugriffstaste. Standardmäßig lautet die Tastenkombination "Strg+Alt+M".

Wenn Sie immer im Vollbildmodus auf das Ziel zugreifen möchten, können Sie den Vollbildmodus als Standardeinstellung auswählen.

So aktivieren Sie den Vollbildmodus als Standardmodus:

1. Klicken Sie auf "Tools" (Extras) > "Options" (Optionen), um das Dialogfeld "Options" (Optionen) zu öffnen.
2. Wählen Sie "Enable Launch in Full Screen Mode" (Start im Vollbildmodus aktivieren), und klicken Sie auf "OK".

Hilfeoptionen

About Raritan Virtual KVM Client (Informationen zum Raritan Virtual KVM Client)

Dieser Menübefehl liefert Versionsinformationen zum Virtual KVM Client, falls Sie Unterstützung durch den technischen Kundendienst von Raritan benötigen.

So rufen Sie die Versionsinformationen ab:

1. Wählen Sie "Help" > "About Raritan Virtual KVM Client" (Hilfe > Informationen zum Raritan Virtual KVM Client) aus.



2. Verwenden Sie die Schaltfläche "Copy to Clipboard" (In Zwischenablage kopieren), um die im Dialogfeld enthaltenen Informationen in eine Zwischenablagedatei zu kopieren, sodass auf diese bei Bedarf später bei Hilfestellung durch den Kundendienst zugegriffen werden kann.

Multi-Platform-Client (MPC)

Der Multi-Platform-Client (MPC) von Raritan ist eine grafische Benutzeroberfläche für die Produktlinien von Raritan, mit der Sie Remotezugriff auf Zielserver erhalten, die mit KVM-über-IP-Geräten von Raritan verbunden sind. Informationen zur Verwendung des MPC finden Sie im Benutzerhandbuch **KVM and Serial Access Clients Guide**, das auf der Raritan-Website auf der gleichen Seite wie das Benutzerhandbuch zur Verfügung steht. Dort finden Sie Anweisungen zum Starten des MPC.

Beachten Sie, dass dieser Client von verschiedenen Raritan-Produkten verwendet wird. Deshalb können in diesem Hilfeabschnitt Verweise auf andere Produkte vorkommen.

Starten des MPC über einen Webbrowser

Wichtig: Unabhängig vom verwendeten Browser müssen Popups für die IP-Adresse des Dominion-Geräts zugelassen werden, damit der MPC geöffnet werden kann.

Wichtig: Nur Mac 10.5 und 10.6 mit einem Intel®-Prozessor können JRE 1.6 ausführen und daher als Client verwendet werden. Mac 10.5.8 unterstützt MPC nicht als Standalone-Client.

1. Geben Sie zum Öffnen des MPC von einem Client, auf dem ein beliebiger unterstützter Browser ausgeführt wird, http://IP-ADRESSE/mpc in die Adresszeile ein, wobei "IP-ADRESSE" die IP-Adresse des Raritan-Geräts ist. Der MPC wird in einem neuen Fenster geöffnet.

   Hinweis: Mit dem Befehl "Alt+Tab" können Sie zwischen verschiedenen Fenstern wechseln (nur auf dem lokalen System).

   Wenn sich der MPC öffnet, werden die Raritan-Geräte, die automatisch erkannt und in Ihrem Subnetz gefunden wurden, im Baumformat im Navigator angezeigt.

2. Wenn Ihr Gerät nicht mit Namen im Navigator aufgelistet ist, fügen Sie es manuell hinzu.

   a. Wählen Sie "Connection" > "New Profile" (Verbindung > Neues Profil) aus. Das Fenster Add Connection (Verbindung hinzufügen) wird geöffnet.

   b. Geben Sie im Fenster "Add Connection" (Verbindung hinzufügen) eine Gerätebeschreibung ein sowie einen Verbindungstyp an, fügen Sie die IP-Adresse des Geräts hinzu und klicken Sie auf OK. Diese Angaben können Sie später bearbeiten.

3. Doppelklicken Sie im Navigatorfenster auf der linken Seite auf das Symbol für Ihr Raritan-Gerät, um eine Verbindung herzustellen.

Hinweis: Je nach Browser und den Browsersicherheitseinstellungen werden möglicherweise verschiedene Meldungen zur Sicherheit und Zertifikatprüfung sowie Warnungsmeldungen angezeigt. Bestätigen Sie die Optionen, um den MPC zu öffnen.

Hinweis: Wenn Sie Firefox 3.0.3 verwenden, kann es zu Problemen beim Starten der Anwendung kommen. Wenn dies der Fall ist, löschen Sie den Browser-Cache und starten Sie die Anwendung erneut.



Kapitel 4 Virtuelle Medien

In diesem Kapitel

Überblick

Virtuelle Medien erweitern die KVM-Funktionen. Sie ermöglichen KVM-Zielservern den Remotezugriff auf Medien auf einem Client-PC und Netzwerkdateiservern. LX unterstützt den Zugriff auf virtuelle Medien auf Festplatten und remote installierte Abbilder.

Die CIMs (Computer Interface Modules) D2CIM-VUSB und D2CIM-DVUSB unterstützen virtuelle Mediensitzungen mit KVM-Zielservern, die über eine USB 2.0-Schnittstelle verfügen. Diese CIMs unterstützen darüber hinaus den Mausmodus "Absolute Mouse Synchronization" (Absolute Maussynchronisierung) sowie Remote-Firmwareaktualisierungen.

Virtuelle Medien bieten die Möglichkeit, Aufgaben extern zu erledigen. Dazu zählen:

- Übertragen von Dateien
- Durchführen von Diagnosen
- Installieren oder Reparieren von Anwendungen
- Vollständiges Installieren des Betriebssystems

Für Windows®-, Mac®- und Linux™-Clients werden die folgenden virtuellen Medientypen unterstützt:

- Interne und per USB angeschlossene CD- und DVD-Laufwerke
- USB-Massenspeichergeräte
- PC-Festplatte
- ISO-Abbilder (Datenträgerabbilder)

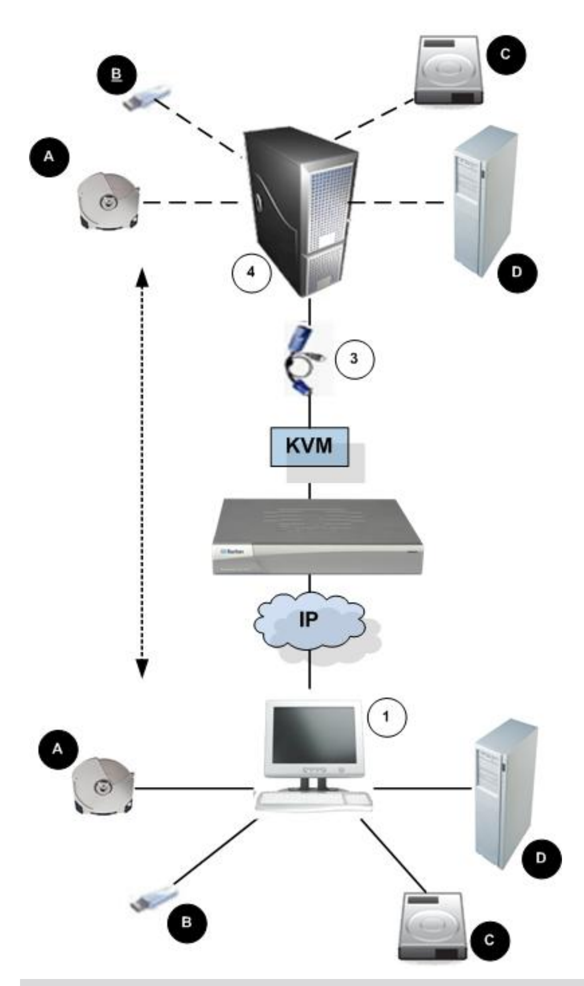
Hinweis: ISO9660 wird standardmäßig von Raritan unterstützt. Andere ISO-Standards können jedoch ebenfalls verwendet werden.

Die folgenden Client-Betriebssysteme werden unterstützt:

- Windows
- Mac OS X 10.5
- Mac OS X 10.6
- Red Hat Desktop 4.0 und 5.0
- Open SUSE 10, 11
- Fedora 13 und 14

Der Virtual KVM Client (VKC) und der Multi-Platform-Client (MPC) können zum Mounten virtueller Medientypen verwendet werden. Eine Ausnahme bildet hierbei Mac OS X 10.5, das nur vom MPC unterstützt wird.





Diagrammschlüssel			
1	Desktop-PC	A	CD-/DVD-Laufwerk
2	LX	B	USB-Massenspeichergerät
3	CIM	C	PC-Festplatte
4	Zielserver	D	Remote-Dateiserver (ISO-Abbilder)

Voraussetzungen für die Verwendung virtueller Medien

Mit dem Feature für virtuelle Medien können Sie bis zu zwei Laufwerke (verschiedenen Typs) installieren, die durch das aktuell dem Zielgerät zugeordnete USB-Profil unterstützt werden. Diese Laufwerke sind während der KVM-Sitzung zugänglich.

Sie können beispielsweise eine bestimmte CD-ROM installieren, verwenden und nach Fertigstellung Ihrer Arbeit wieder trennen. Der virtuelle Medienkanal für CD-ROMs bleibt jedoch offen, sodass Sie eine andere CD-ROM virtuell installieren können. Diese virtuellen Medienkanäle bleiben offen, bis die KVM-Sitzung geschlossen wird (vorausgesetzt, sie werden vom USB-Profil unterstützt).

Um das virtuelle Medium zu verwenden, schließen Sie es an den Client-PC oder Netzwerkdateiserver an, auf den Sie über den Zielserver zugreifen möchten. Dieser Schritt muss nicht als erster erfolgen, jedoch bevor Sie versuchen, auf das Medium zuzugreifen.

Für die Verwendung virtueller Medien müssen folgende Bedingungen erfüllt sein:

Dominion-Gerät

- Für Benutzer, die Zugriff auf virtuelle Medien benötigen, müssen die Geräteberechtigungen für den Zugriff auf die relevanten Ports sowie der virtuelle Medienzugriff (Portberechtigung VM Access [VM-Zugriff]) für diese Ports eingerichtet werden. Portberechtigungen werden auf Gruppenebene eingerichtet.
- Zwischen dem Gerät und dem Zielserver muss eine USB-Verbindung bestehen.
- Wenn Sie die PC-Freigabe verwenden möchten, müssen die Security Settings (Sicherheitseinstellungen) auf der Seite "Security Settings" (Sicherheitseinstellungen) aktiviert sein. **Optional**
- Sie müssen das richtige USB-Profil für den KVM-Zielserver auswählen, zu dem Sie eine Verbindung herstellen.

Client-PC

- Für bestimmte virtuelle Medienoptionen sind Administratorrechte auf dem Client-PC erforderlich (z. B. Umleitung ganzer Laufwerke).

Hinweis: Wenn Sie Windows Vista or Windows 7 verwenden, deaktivieren Sie "User Account Control" (Benutzerkontensteuerung), oder wählen Sie beim Start von Internet Explorer "Run as Administrator" (Als Administrator ausführen) aus. Klicken Sie dazu auf das Menü "Start", klicken Sie mit der rechten Maustaste auf "Internet Explorer", und wählen Sie "Run as Administrator" (Als Administrator ausführen) aus.



Zielserver

- KVM-Zielserver müssen über USB angeschlossene Laufwerke unterstützen.
- Auf KVM-Zielservern mit Windows 2000 müssen alle aktuellen Patches installiert sein.
- USB 2.0-Ports sind schneller und daher vorzuziehen.



Virtuelle Medien in einer Linux-Umgebung

Die folgenden Informationen zur Verwendung von virtuellen Medien sind für Linux®-Benutzer relevant.

Erforderliche Stammbenutzerberechtigung

- Ihre virtuelle Medienverbindung wird ggf. beendet, wenn Sie ein CD-ROM-Laufwerk von einem Linux-Client auf einem Ziel bereitstellen und anschließend die Bereitstellung des CD-ROM-Laufwerks aufheben. Die Verbindung wird auch beendet, wenn ein Diskettenlaufwerk bereitgestellt wurde und dann eine Diskette entnommen wird. Um diese Probleme zu vermeiden, melden Sie sich als Stammbenutzer an.

Berechtigungen

Zum Verbinden des Laufwerks bzw. der CD-ROM mit dem Ziel müssen Benutzer über die entsprechenden Zugriffsberechtigungen verfügen. Dies kann mit folgenden Befehlen geprüft werden:

```
guest_user@administrator-desktop:~$ ls -l /dev/sr0

brw-rw----+ 1 root cdrom 11, 12-03-2010 11:52 /dev/sr0
```

Im obigen Beispiel muss die Berechtigung geändert werden und Lesezugriff gewährt werden.

In einem System, das Zugriffssteuerungslisten in seinen Dateidienstprogrammen unterstützt, ändert der Befehl "Is" (Ist) seine Funktionsweise wie folgt:

- Für Dateien, die eine Standard-Zugriffssteuerungsliste oder eine Zugriffssteuerungsliste mit mehr als den drei erforderlichen ACL-Einträgen enthalten, zeigt das Dienstprogramm "Is(1)" (Ist (1))" in der langen von "Is -I" (Is -I) erzeugten Form ein Pluszeichen (+) nach der Berechtigungszeichenfolge an.

Dies wird im Beispiel oben für "/dev/sr0, use getfacl –a /dev/sr0" angegeben, um festzustellen, ob der Benutzer im Rahmen einer Zugriffssteuerungsliste Zugriff erhalten hat. In diesem Fall trifft dies zu, sodass der Benutzer eine Verbindung mit der CD-ROM zum Ziel herstellen kann, auch wenn die Ausgabe des Befehls "ls -l" (Ist -I) gegenteilig lautet.



```
guest_user@administrator-desktop:~$ getfacl -a /dev/sr0
getfacl: Removing leading '/' from absolute path names
# file: dev/sr0
# owner: root
# group: cdrom
user::rw-
user:guest_user:rw-
group::rw-
mask::rw-
other::---
```

Eine ähnliche Prüfung der Berechtigungen für ein Wechselmedium ergibt Folgendes:

```
guest_user@administrator-desktop:~$ ls -l /dev/sdb1
brw-rw---- 1 root disk 8, 17 12-03-2010 12:02 /dev/sdb1

guest_user@administrator-desktop:~$ ls -l /dev/sdb1
brw-rw---- 1 root disk 8, 17 12-03-2010 12:02 /dev/sdb1
&gt;  getfacl -a /dev/sdb1
getfacl: Removing leading '/' from absolute path names
# file: dev/sdb1
# owner: root
# group: disk
user::rw-
group::rw-
other::---
```

Dies erfordert, dass der Benutzer schreibgeschützten Zugriff auf das Wechselmedium erhält:

```
root@administrator-desktop:~# chmod 664 /dev/sdb1
root@administrator-desktop:~# ls -l /dev/sdb1
brw-rw-r-- 1 root disk 8, 17 12-03-2010 12:02 /dev/sdb1
```

Das Laufwerk steht dann für die Verbindung mit dem Ziel zur Verfügung.



Fälle, in denen Lese-/Schreibzugriff nicht verfügbar ist

Der Lese-/Schreibzugriff auf virtuelle Medien ist in den folgenden Situationen nicht verfügbar:

- Für Linux®- und Mac®-Clients
- Bei allen Festplatten
- Wenn das Laufwerk schreibgeschützt ist
- Wenn der Benutzer nicht über eine Lese-/Schreibberechtigung verfügt.
  - Unter **Port Permission** (Port-Berechtigung) ist für **Access** (Zugriff) die Einstellung **None** (Kein) oder **View** (Anzeigen) ausgewählt.
  - Unter **Port Permission** (Port-Berechtigung) ist für **VM Access** (VM-Zugriff) die Einstellung **Read-Only** (Schreibgeschützt) oder **Deny** (Ablehnen) ausgewählt.

Verwenden virtueller Medien

Lesen Sie die Hinweise zu den ***Voraussetzungen für die Verwendung virtueller Medien*** (auf Seite 98), bevor Sie virtuelle Medien verwenden.

So verwenden Sie virtuelle Medien:

1. Wenn Sie auf Dateiserver-ISO-Abbilder zugreifen möchten, lassen Sie diese Dateiserver und Abbilder über die Seite "Remote Console File Server Setup" (Remotekonsolen-Dateiserver-Setup) erkennen. Siehe ***Dateiserver-Setup für virtuelle Medien (nur für Dateiserver-ISO-Abbilder)*** (auf Seite 103).

   Hinweis: Das ISO9660-Format wird standardmäßig von Raritan unterstützt. Andere CD-ROM-Erweiterungen funktionieren ggf. jedoch auch.

2. Öffnen Sie eine KVM-Sitzung mit dem entsprechenden Zielserver.
   a. Rufen Sie über die Remotekonsole die Seite "Port Access" (Portzugriff) auf.
   b. Stellen Sie auf dieser Seite eine Verbindung mit dem Zielserver her:
   - Klicken Sie unter "Port Name" (Portname) auf den entsprechenden Server.
   - Wählen Sie im Menü "Port Action" (Portaktion) den Befehl "Connect" (Verbinden) aus. Der Zielserver wird in einem Fenster des Virtual KVM Client geöffnet.
3. Stellen Sie eine Verbindung mit dem virtuellen Medium her.



Virtuelles Medium	Entsprechende VM-Option
Lokale Laufwerke	Connect Drive (Laufwerk verbinden)
Lokale CD-/DVD-Laufwerke	"Connect CD-ROM/ISO" (CD-ROM/ISO verbinden)
ISO-Abbilder	"Connect CD-ROM/ISO" (CD-ROM/ISO verbinden)
Dateiserver-ISO-Abbilder	"Connect CD-ROM/ISO" (CD-ROM/ISO verbinden)

Nach Abschluss Ihrer Aufgaben trennen Sie die Verbindung zum virtuellen Medium. Siehe ***Trennen von virtuellen Medien*** (auf Seite 109)

Dateiserver-Setup für virtuelle Medien (nur für Dateiserver-ISO-Abbilder)

Hinweis: Dieses Feature ist nur für den Zugriff auf Dateiserver-ISO-Abbilder über virtuelle Medien erforderlich. Das ISO9660-Format wird standardmäßig von Raritan unterstützt. Andere CD-ROM-Erweiterungen funktionieren ggf. jedoch auch.

Hinweis: Der Dateiserver muss SMB/CIFS unterstützen.

Legen Sie auf der Seite "File Server Setup" (Dateiserver-Setup) der Remotekonsole die Dateiserver und Abbildpfade fest, auf die Sie über virtuelle Medien zugreifen möchten. Hier angegebene Dateiserver-ISO-Abbilder stehen im Dialogfenster "Map Virtual Media CD/ISO Image" (CD-/ISO-Abbild als virtuelles Medium zuordnen) unter "Remote Server ISO Image" (ISO-Abbild auf Remoteserver) in den Dropdownlisten "Hostname" und "Image" (Abbild) zur Auswahl. Siehe ***Mounten von CD-ROM-/DVD-ROM-/ISO-Abbildern*** (siehe "***Installieren von CD-ROM-/DVD-ROM-/ISO-Abbildern***" auf Seite 107).

So legen Sie Dateiserver-ISO-Abbilder für den virtuellen Medienzugriff fest:

1. Wählen Sie in der Remotekonsole "Virtual Media" (Virtuelle Medien) aus. Die Seite "File Server Setup" (Dateiserver-Setup) wird angezeigt.
2. Aktivieren Sie das Kontrollkästchen "Selected" (Ausgewählt) für alle Medien, die als virtuelle Medien zugänglich sein sollen.
3. Geben Sie Informationen zu den Dateiserver-ISO-Abbildern ein, auf die Sie zugreifen möchten:
   - IP Address/Host Name (IP-Adresse/Hostname) – Hostname oder IP-Adresse des Dateiservers.



- Image Path (Abbildpfad) – Vollständiger Pfad zum Speicherort des ISO-Abbildes. Zum Beispiel /sharename0/path0/image0.iso, \sharename1\path1\image1.iso usw.

Hinweis: Der Hostname darf aus maximal 232 Zeichen bestehen.

4. Klicken Sie auf "Save" (Speichern). Alle hier angegebenen Medien stehen nun im Dialogfeld Map Virtual Media CD/ISO Image (CD-/ISO-Abbild als virtuelles Medium zuordnen) zur Auswahl.

Hinweis: Aufgrund von technischen Einschränkungen der Drittanbieter-Software des LX-, KX-, KSX- oder KX101 G2-Geräts können Sie bei Verwendung einer IPv6-Adresse nicht über virtuelle Medien auf ein Remote-ISO-Abbild zugreifen.

Hinweis: Wenn Sie eine Verbindung zu einem Windows 2003®-Server herstellen und versuchen, ein ISO-Abbild vom Server zu laden, ist es möglich, dass Sie die Fehlermeldung "Virtual Media mounting on port failed. Unable to connect to the file server or incorrect File Server username and password". (Installation der virtuellen Medien auf Port fehlgeschlagen. Verbindung mit Dateiserver konnte nicht hergestellt werden oder falsches Kennwort bzw. falschen Benutzernamen für Dateiserver verwendet.) angezeigt bekommen. Falls dies eintritt, deaktivieren Sie unter den Richtlinien für den Domänen-Controller die Option "Microsoft Network Server: Digitally Sign Communications" (Microsoft-Netzwerk [Server]: Kommunikation digital signieren).

Hinweis: Wenn Sie eine Verbindung zu einen Windows 2003-Server herstellen und versuchen, ein ISO-Abbild vom Server zu laden, ist es möglich, dass Sie die Fehlermeldung "Virtual Media mounting on port failed. Unable to connect to the file server or incorrect File Server username and password". (Installation der virtuellen Medien auf Port fehlgeschlagen. Verbindung mit Dateiserver konnte nicht hergestellt werden oder falsches Kennwort bzw. falschen Benutzernamen für Dateiserver verwendet.) angezeigt bekommen. Falls dies eintritt, deaktivieren Sie unter den Richtlinien für den Dömänen-Controller die Option "Microsoft Network Server: Digitally Sign Communications" (Microsoft-Netzwerk [Server]: Kommunikation digital signieren).



Herstellen einer Verbindung mit virtuellen Medien

Installieren von lokalen Laufwerken

Mit dieser Option installieren Sie ein gesamtes Laufwerk. Das gesamte Festplattenlaufwerk wird auf dem Zielserver virtuell installiert. Verwenden Sie diese Option nur für Festplatten und externe Laufwerke. Netzwerklaufwerke, CD-ROM- oder DVD-ROM-Laufwerke sind nicht enthalten. Nur für diese Option ist "Read/Write" (Lese-/Schreibzugriff) verfügbar.

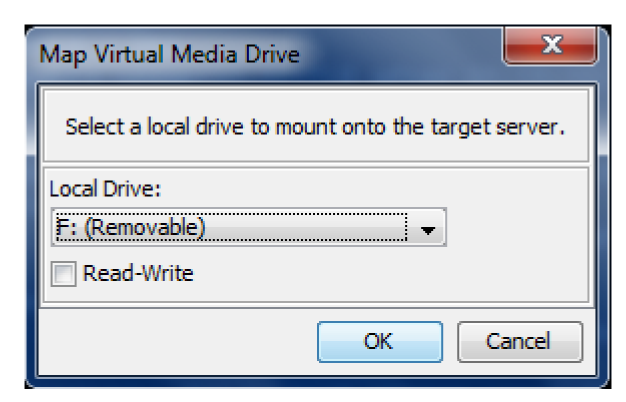
Hinweis: KVM-Zielserver mit bestimmten Versionen des Windows-Betriebssystems akzeptieren möglicherweise keine neuen Massenspeicherverbindungen, nachdem eine NTFS-formatierte Partition (z. B. das lokale Laufwerk C) an sie umgeleitet wurde.

Schließen Sie in diesem Fall die Remotekonsole, und stellen Sie erneut eine Verbindung her, bevor Sie ein weiteres virtuelles Mediengerät umleiten. Wenn andere Benutzer mit demselben Zielserver verbunden sind, müssen auch sie diese Verbindung trennen.

Hinweis: Mounten Sie beim KX II 2.1.0 (und höher) ein externes Laufwerk, z. B. ein Diskettenlaufwerk, so leuchtet die LED permanent, da das Gerät alle 500 Millisekunden prüft, ob das Laufwerk noch installiert ist.

So greifen Sie auf ein Laufwerk auf dem Client-Computer zu:

1. Wählen Sie im Virtual KVM Client **Virtual Media > Connect Drive** (Virtuelle Medien > Laufwerk verbinden). Das Dialogfeld **Map Virtual Media Drive** (Virtuelles Medienlaufwerk zuordnen) wird angezeigt. ()



2. Wählen Sie das entsprechende Laufwerk in der Dropdown-Liste **Local Drive** (Lokales Laufwerk) aus.

3. Für den Lese- und Schreibzugriff müssen Sie das Kontrollkästchen "Read-Write" (Lese-/Schreibzugriff) aktivieren. Diese Option steht nur für Wechsellaufwerke zur Verfügung. Weitere Informationen finden Sie unter ***Fälle, in denen Lese-/Schreibzugriff nicht verfügbar ist*** (auf Seite 102). Bei dieser Option können Sie Daten auf dem angeschlossenen USB-Datenträger lesen und schreiben.

WARNUNG: Den Lese-/Schreibzugriff zu aktivieren kann gefährlich sein! Wenn mehrere Einheiten gleichzeitig auf dasselbe Laufwerk zugreifen, kann dies zu Datenbeschädigungen führen. Sollten Sie den Schreibzugriff nicht benötigen, deaktivieren Sie dieses Kontrollkästchen.

---

4. Klicken Sie auf "Connect" (Verbinden). Das Medium wird auf dem Zielserver virtuell installiert. Sie können darauf wie auf jedes andere Laufwerk zugreifen.



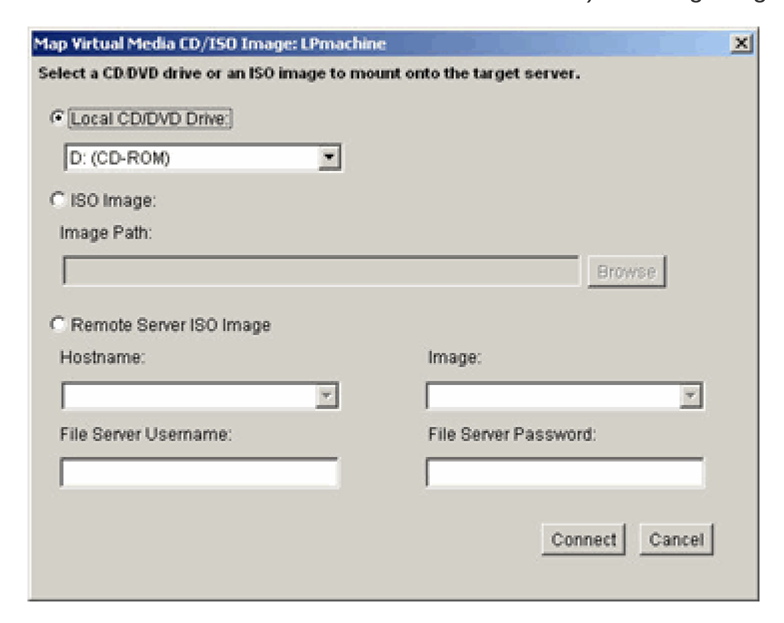
Installieren von CD-ROM-/DVD-ROM-/ISO-Abbildern

Mit dieser Option installieren Sie CD-ROM-, DVD-ROM- und ISO-Abbilder.

Hinweis: Das ISO9660-Format wird standardmäßig von Raritan unterstützt. Andere CD-ROM-Erweiterungen funktionieren ggf. jedoch auch.

So greifen Sie auf ein CD-ROM-, DVD-ROM- oder ISO-Abbild zu:

1. Wählen Sie im Virtual KVM Client "Virtual Media > Connect CD-ROM/ISO Image" (Virtuelle Medien > CD-ROM-/ISO-Abbild verbinden). Das Dialogfeld "Map Virtual Media CD/ISO Image" (CD-/ISO-Abbild als virtuelles Medium zuordnen) wird angezeigt.



2. Gehen Sie bei internen und externen CD-ROM- und DVD-ROM-Laufwerken folgendermaßen vor:
   a. Wählen Sie die Option "Local CD/DVD Drive" (Lokales CD-/DVD-Laufwerk).
   b. Wählen Sie das entsprechende Laufwerk in der Dropdown-Liste "Local CD/DVD Drive" (Lokales CD-/DVD-Laufwerk) aus. Diese Liste enthält alle verfügbaren internen und externen CD- und DVD-Laufwerksnamen.
   c. Klicken Sie auf "Connect" (Verbinden).
3. Gehen Sie bei ISO-Abbildern folgendermaßen vor:
   a. Wählen Sie die Option "ISO Image" (ISO-Abbild). Mit dieser Option greifen Sie auf ein Laufwerkabbild einer CD, DVD oder Festplatte zu. Nur das ISO-Format wird unterstützt.

b. Klicken Sie auf "Browse" (Durchsuchen).

c. Navigieren Sie zu dem Pfad des gewünschten Laufwerkabbilds, und klicken Sie auf "Open" (Öffnen). Der Pfad wird in das Feld "Image Path" (Abbildpfad) geladen.

d. Klicken Sie auf "Connect" (Verbinden).

4. Gehen Sie bei Remote-ISO-Abbildern auf einem Dateiserver folgendermaßen vor:

   a. Wählen Sie die Option "Remote Server ISO Image" (ISO-Abbild auf Remoteserver).

   b. Wählen Sie in der Dropdown-Liste einen Hostnamen und ein Abbild aus. Zur Verfügung stehen die Dateiserver und Abbildpfade, die Sie auf der Seite "File Server Setup" (Dateiserver-Setup) konfiguriert haben. Die Dropdown-Liste enthält nur Elemente, die Sie auf der Seite "File Server Setup" (Dateiserver-Setup) konfiguriert haben.

   c. "File Server Username" (Dateiserver-Benutzername) – Der für den Zugriff auf den Dateiserver erforderliche Benutzername. Der Name darf den Domänennamen, wie z. B. meinedomäne/Benutzername, enthalten.

   d. "File Server Password" (Dateiserver-Kennwort) – Das für den Zugriff auf den Dateiserver erforderliche Kennwort (Eingabe erfolgt verdeckt).

   e. Klicken Sie auf "Connect" (Verbinden).

   Das Medium wird auf dem Zielserver virtuell installiert. Sie können darauf wie auf jedes andere Laufwerk zugreifen.

Hinweis: Wenn Sie Dateien auf einem Linux®-Ziel bearbeiten, verwenden Sie den Befehl "Linux Sync" (Linux-Synchronisierung), nachdem die Dateien mithilfe eines virtuellen Mediums kopiert wurden, um die kopierten Dateien anzuzeigen. Die Dateien werden möglicherweise erst angezeigt, nachdem die Synchronisierung durchgeführt wurde.

Hinweis: Wenn Sie mit dem Windows 7®-Betriebssystem® arbeiten, werden Wechseldatenträger nicht standardmäßig im Windows-Ordner "Arbeitsplatz" angezeigt, sobald Sie ein lokales CD-/DVD-Laufwerk oder ein lokales oder Remote-ISO-Abbild mounten. Um das lokale CD-/DVD-Laufwerk oder das lokale oder Remote-ISO-Abbild in diesem Ordner anzuzeigen, wählen Sie "Extras" > "Ordneroptionen" > "Ansicht" aus und deaktivieren die Option "Leere Laufwerke im Ordner "Computer" ausblenden".

Hinweis: Aufgrund von technischen Einschränkungen der Drittanbieter-Software können Sie bei Verwendung einer IPv6-Adresse nicht über virtuelle Medien auf ein Remote-ISO-Abbild zugreifen.



Trennen von virtuellen Medien

So trennen Sie virtuelle Medienlaufwerke:

- Wählen Sie für lokale Laufwerke "Virtual Media" > "Disconnect Drive" (Virtuelle Medien > Laufwerk trennen) aus.
- Wählen Sie für CD-ROM-, DVD-ROM- und ISO-Abbilder "Virtual Media > Disconnect CD-ROM/ISO Image" (Virtuelle Medien > CD-ROM-/ISO-Abbild trennen) aus.

Hinweis: Anstatt das virtuelle Medium über den Befehl "Disconnect" (Trennen) zu trennen, können Sie auch einfach die KVM-Verbindung beenden.

Kapitel 5 User Management (Benutzerverwaltung)

In diesem Kapitel

Benutzergruppen

LX speichert eine interne Liste aller Benutzer- und Gruppennamen, um die Zugriffsautorisierung und die Berechtigungen festzulegen. Diese Informationen werden intern in einem verschlüsselten Format gespeichert. Es gibt verschiedene Arten der Authentifizierung. Diese wird als lokale Authentifizierung bezeichnet. Alle Benutzer müssen authentifiziert werden. Wenn LX für LDAP/LDAPS oder RADIUS konfiguriert wurde, wird erst deren entsprechende Authentifizierung durchgeführt und anschließend die lokale Authentifizierung.

Jedes LX enthält standardmäßig drei Benutzergruppen. Diese Gruppen können nicht gelöscht werden:

Benutzer	Beschreibung
Admin	Benutzer dieser Gruppe verfügen über vollständige Administratorrechte. Der ursprüngliche werkseitige Standardbenutzer ist Mitglied dieser Gruppe und verfügt über sämtliche Systemrechte. Außerdem muss der Benutzer "Admin" der Gruppe "Admin" angehören.
Unknown (Unbekannt)	Dies ist die Standardgruppe für Benutzer, die extern über LDAP/LDAPS oder RADIUS authentifiziert werden oder die im System unbekannt sind. Wenn der externe LDAP/LDAPS- oder RADIUS-Server keine gültige Benutzergruppe erkennt, wird die Gruppe "Unknown" (Unbekannt) verwendet. Außerdem wird jeder neu erstellte Benutzer automatisch in diese Gruppe aufgenommen, bis der Benutzer einer anderen Gruppe zugewiesen wird.
Individual Group (Individuelle Gruppe)	Eine individuelle Gruppe ist im Prinzip eine aus einer Person bestehende "Gruppe". Dies bedeutet, dass sich der Benutzer in seiner eigenen Gruppe befindet und nicht mit anderen echten Gruppen verknüpft ist. Individuelle Gruppen können Sie am @-Zeichen im Gruppennamen erkennen. In individuellen Gruppen können Benutzerkonten dieselben Rechte wie eine



	Gruppe aufweisen.

In LX können bis zu 254 Benutzergruppen erstellt werden. In LX können bis zu 254 Benutzergruppen erstellt werden.

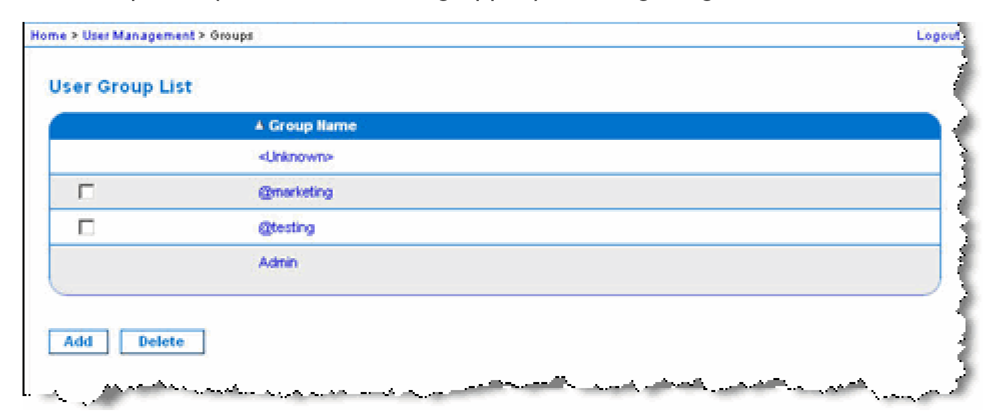
User Group List (Liste der Benutzergruppen)

Benutzergruppen werden bei der lokalen und der Remoteauthentifizierung (über RADIUS oder LDAP/LDAPS) verwendet. Es ist empfehlenswert, Benutzergruppen vor dem Erstellen einzelner Benutzer zu definieren, da jeder Benutzer einer vorhandenen Benutzergruppe hinzugefügt werden muss.

Die Seite "User Group List" (Liste der Benutzergruppen) enthält eine Liste aller Benutzergruppen, die in auf- oder absteigender Reihenfolge sortiert werden kann, indem Sie auf die Spaltenüberschrift "Group Name" (Gruppenname) klicken. Auf der Seite "User Group List" (Liste der Benutzergruppen) können Sie außerdem Benutzergruppen hinzufügen, ändern oder löschen.

▶ So zeigen Sie eine Liste der Benutzergruppen an:

- Wählen Sie "User Management > User Group List" (Benutzerverwaltung > Liste der Benutzergruppen). Die Seite "User Group List" (Liste der Benutzergruppen) wird angezeigt.



Beziehung zwischen Benutzern und Gruppen

Benutzer sind Mitglied in einer Gruppe, und Gruppen verfügen über bestimmte Berechtigungen. Sie können Zeit sparen, indem Sie die verschiedenen Benutzer Ihrer LX-Einheit in Gruppen organisieren. So können Sie die Berechtigungen aller Benutzer in einer Gruppe auf einmal verwalten anstatt für jeden Benutzer einzeln.

Sie können bei Bedarf auch darauf verzichten, bestimmte Benutzer Gruppen zuzuordnen. In diesem Fall können Sie den Benutzer als "Individuell" klassifizieren.

Nach der erfolgreichen Authentifizierung verwendet das Gerät Gruppeninformationen, um die Berechtigungen des Benutzers zu bestimmen, z. B. die Zugriffsberechtigungen für verschiedene Server-Ports, ob ein Neustart des Geräts zulässig ist und weitere Funktionen.

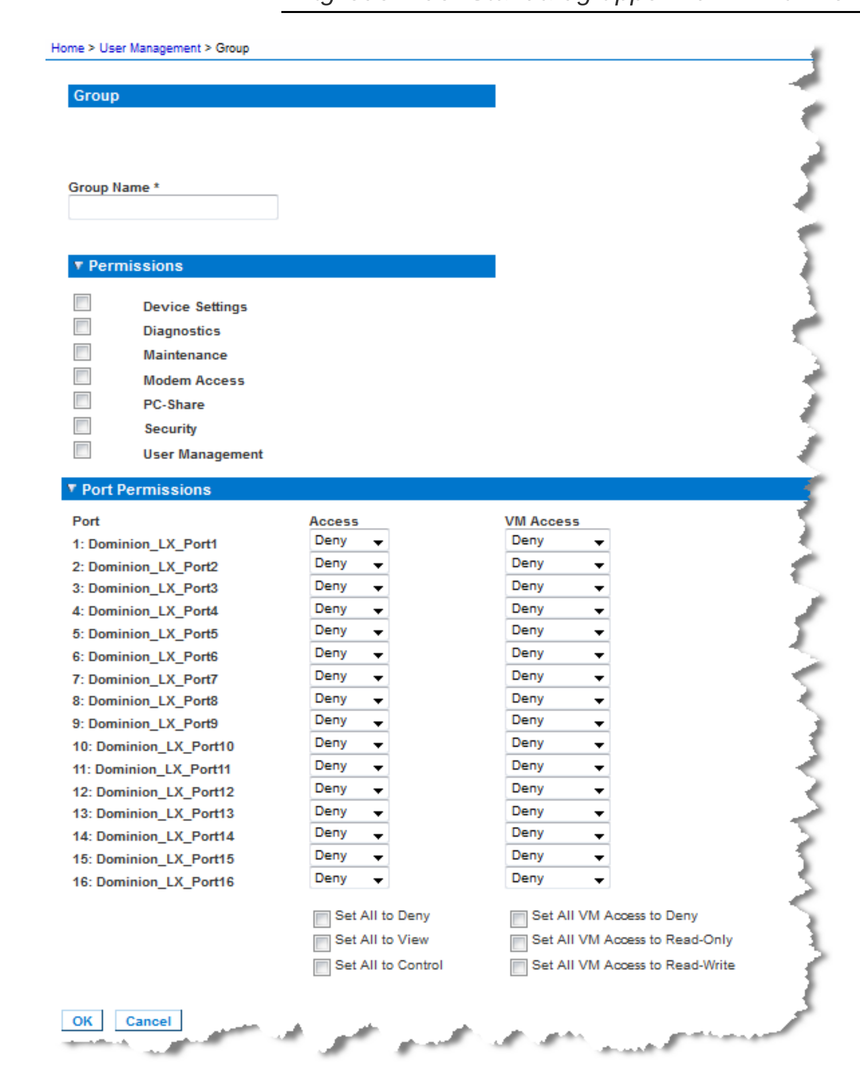
Hinzufügen einer neuen Benutzergruppe

► **So fügen Sie eine neue Benutzergruppe hinzu:**

1. Wählen Sie "User Management > Add New User Group" (Benutzerverwaltung > Neue Benutzergruppe hinzufügen) oder klicken Sie auf der Seite "User Group List" (Liste der Benutzergruppen) auf die Schaltfläche "Add" (Hinzufügen).
2. Geben Sie im Feld "Group Name" (Gruppenname) einen aussagekräftigen Namen für die neue Benutzergruppe ein (bis zu 64 Zeichen).
3. Aktivieren Sie die Kontrollkästchen neben den Berechtigungen, die Sie allen Benutzern in dieser Gruppe gewähren möchten. Siehe ***Festlegen von Berechtigungen*** (auf Seite 113).
4. Klicken Sie auf OK.



Hinweis: Im MPC und auf der lokalen LX-Konsole sind viele administrative Funktionen verfügbar. Diese Funktionen stehen nur Mitgliedern der Standardgruppe "Admin" zur Verfügung.



Festlegen von Berechtigungen

Wichtig: Wenn das Kontrollkästchen "User Management" (Benutzerverwaltung) aktiviert ist, können Mitglieder der Gruppe die Berechtigungen aller Benutzer einschließlich ihrer eigenen ändern. Lassen Sie beim Zuordnen dieser Berechtigungen Vorsicht walten.

Berechtigung	Beschreibung
Device Settings (Geräteeinstellungen)	Netzwerkeinstellungen, Einstellungen für Datum und Uhrzeit, Portkonfiguration (Kanalnamen usw.), Ereignisverwaltung



Berechtigung	Beschreibung
	(SNMP, Syslog), Dateiserver-Setups für virtuelle Medien
Diagnose	Status der Netzwerkschnittstelle, Netzwerkstatistik, Ping an den Host, Verfolgen der Route zum Host, LX-Diagnose.
Wartung	Sichern und Wiederherstellen von Datenbanken, Firmware-Aktualisierung, Wiederherstellen der Standardeinstellungen, Neustart.
Modem Access (Modemzugriff)	Berechtigung zur Verwendung des Modems, um eine Verbindung zum LX-Gerät herzustellen
PC-Share (PC-Freigabe)	Gleichzeitiger Zugriff auf ein Zielgerät durch mehrere Benutzer. Wenn Sie eine Schichtkonfiguration verwenden, in der ein LX-Basisgerät für den Zugriff auf mehrere andere Schichtgeräte verwendet wird, müssen alle Geräte dieselben PC-Freigabeeinstellung verwenden. Weitere Informationen zu Schichten finden Sie unter ***Konfigurieren und Aktivieren von Schichten*** (auf Seite 142).
Security (Sicherheit)	SSL-Zertifikat, Sicherheitseinstellungen (VM-Freigabe, PC-Freigabe).
User Management (Benutzerverwaltung)	Benutzer- und Gruppenverwaltung, Remoteauthentifizierung (LDAP/LDAPS/RADIUS), Anmeldeeinstellungen. Wenn Sie eine Schichtkonfiguration verwenden, in der ein LX-Basisgerät für den Zugriff auf mehrere andere Schichtgeräte verwendet wird, müssen auf allen Geräten dieselben Einstellungen für Benutzer, Benutzergruppe und Remote-Authentifizierung verwendet werden. Weitere Informationen zu Schichten finden Sie unter ***Konfigurieren und Aktivieren von Schichten*** (auf Seite 142).



Festlegen von Port-Berechtigungen

Sie können für jeden Serverport den Zugriffstyp der Gruppe sowie den Portzugriffstyp auf virtuelle Medien festlegen. Die Standardeinstellung für alle Berechtigungen ist "Deny" (Ablehnen).

Portzugriff

Option	Beschreibung
"Deny" (Ablehnen)	Zugriff vollständig verweigert
"View" (Anzeigen)	Anzeigen des Videobildes, aber keine Interaktion mit dem angeschlossenen Zielserver.
"Control" (Steuern)	Steuerung des angeschlossenen Zielservers. Steuerung muss bei VM der Gruppe zugewiesen sein. Damit alle Benutzer in einer Benutzergruppe hinzugefügte KVM-Switches erkennen können, muss jedem Benutzer Steuerzugriff gewährt werden. Benutzer ohne diese Berechtigung können einen KVM-Switch, der später hinzugefügt wird, nicht anzeigen.

VM-Zugriff

Option	Beschreibung
"Deny" (Ablehnen)	Berechtigung für virtuelle Medien wird für diesen Port vollständig verweigert.
"Read-Only" (Lese-zugriff)	Zugriff auf virtuelle Medien ist auf das Lesen beschränkt.
"Read-Write" (Lese-/Schreibzugriff)	Vollständiger Zugriff (Lesen und Schreiben) auf virtuelle Medien.

Wenn Sie eine Schichtkonfiguration verwenden, in der ein LX-Basisgerät für den Zugriff auf mehrere andere Schichtgeräte verwendet wird, erzwingt das Schichtgerät individuelle Portsteuerungsebenen. Weitere Informationen zu Schichten finden Sie unter ***Konfigurieren und Aktivieren von Schichten*** (auf Seite 142).



Festlegen von Berechtigungen für eine individuelle Gruppe

So legen Sie Berechtigungen für eine individuelle Benutzergruppe fest:

1. Wählen Sie die gewünschte Gruppe aus der Liste der Gruppen aus. Individuelle Gruppen können Sie am @-Zeichen im Gruppennamen erkennen.
2. Klicken Sie auf den Gruppennamen. Die Seite "Group" (Gruppe) wird angezeigt.
3. Wählen Sie die gewünschten Berechtigungen aus.
4. Klicken Sie auf "OK".

Ändern einer vorhandenen Benutzergruppe

Hinweis: Für die Gruppe Admin sind alle Berechtigungen aktiviert und dies kann nicht geändert werden.

So ändern Sie eine vorhandene Benutzergruppe:

1. Bearbeiten Sie auf der Seite "Group" (Gruppe) die entsprechenden Felder, und legen Sie die gewünschten Berechtigungen fest.
2. Legen Sie unter "Permissions" (Berechtigungen) die Berechtigungen für die Gruppe fest. Aktivieren Sie die Kontrollkästchen für die Berechtigungen, die Sie allen Benutzern in dieser Gruppe gewähren möchten. Siehe ***Festlegen von Berechtigungen*** (auf Seite 113).
3. Legen Sie unter "Port Permissions" (Port-Berechtigungen) die Port-Berechtigungen fest. Legen Sie die für die Benutzer in dieser Gruppe zugänglichen Server-Ports fest, und geben Sie die Zugriffsart an. Siehe ***Festlegen von Portberechtigungen*** (siehe "***Festlegen von Port-Berechtigungen***" auf Seite 115).
4. Klicken Sie auf "OK".

So löschen Sie eine Benutzergruppe:

Wichtig: Wenn Sie eine Gruppe mit Benutzern löschen, werden die Benutzer automatisch der Benutzergruppe "<unknown>"(Unbekannt) zugewiesen.

Tipp: Um herauszufinden, welche Benutzer einer bestimmten Gruppe angehören, sortieren Sie die Benutzerliste nach Benutzergruppe.

1. Wählen Sie eine Gruppe aus der Liste aus, indem Sie das Kontrollkästchen links vom Gruppennamen aktivieren.
2. Klicken Sie auf "Delete" (Löschen).



3. Klicken Sie zum Bestätigen des Löschvorgangs auf "OK".

Benutzer

Benutzern müssen Benutzernamen und Kennwörter zugeordnet werden, damit sie auf LX zugreifen können. Anhand dieser Informationen werden Benutzer authentifiziert, die versuchen, auf LX zuzugreifen. Für jede Benutzergruppe können bis zu 254 Benutzer erstellt werden.

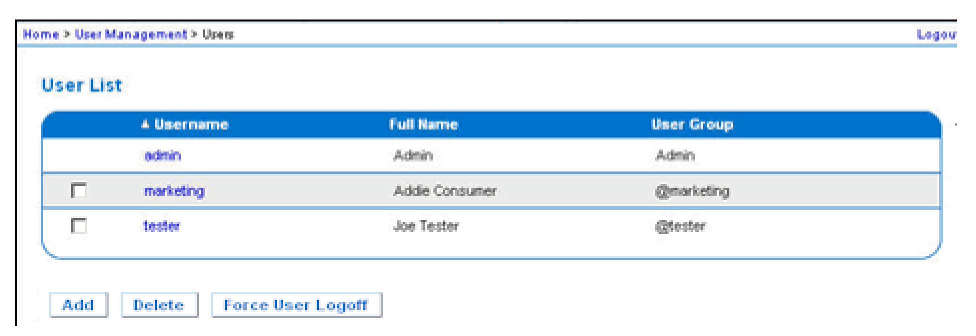
Wenn Sie eine Schichtkonfiguration verwenden, in der ein LX-Basisgerät für den Zugriff auf mehrere andere Schichtgeräte verwendet wird, benötigen Benutzer die Zugriffsberechtigung für das Basisgerät sowie auf das individuelle Schichtgerät (bei Bedarf). Wenn sich Benutzer am Basisgerät anmelden, wird jedes Schichtgerät abgefragt und der Benutzer kann auf jeden Zielserver zugreifen, für den er Berechtigungen aufweist. Weitere Informationen zu Schichten finden Sie unter ***Konfigurieren und Aktivieren von Schichten*** (auf Seite 142).

User List (Benutzerliste)

Die Seite "User List" (Benutzerliste) enthält eine Liste aller Benutzer einschließlich des Benutzernamens, des vollständigen Namens und der Benutzergruppe. Klicken Sie auf einen Spaltennamen, um die Liste nach einer der Spalten zu sortieren. Auf der Seite "User List" (Benutzerliste) können Sie außerdem Benutzer hinzufügen, ändern oder löschen.

▶ So zeigen Sie die Benutzerliste an:

- Wählen Sie "User Management" > "User List" (Benutzerverwaltung > Benutzerliste) aus. Die Seite "User List" (Benutzerliste) wird angezeigt.



Hinzufügen eines neuen Benutzers

Es ist empfehlenswert, Benutzergruppen vor dem Erstellen von LX-Benutzern zu definieren, da jeder Benutzer einer vorhandenen Benutzergruppe zugewiesen werden muss. Siehe **Hinzufügen einer neuen Benutzergruppe** (auf Seite 112).

Auf der Seite "User" (Benutzer) können Sie neue Benutzer hinzufügen, Benutzerinformationen ändern und deaktivierte Benutzer erneut aktivieren.

Hinweis: Ein Benutzername kann deaktiviert werden, wenn die Anzahl der fehlgeschlagenen Anmeldeversuche die auf der Seite "Security Settings" (Sicherheitseinstellungen) festgelegte maximale Anzahl der Anmeldeversuche überschritten hat. Siehe Sicherheitseinstellungen.

So fügen Sie einen neuen Benutzer hinzu:

1. Wählen Sie "User Management > Add New User" (Benutzerverwaltung > Neuen Benutzer hinzufügen) oder klicken Sie auf der Seite "User List" (Benutzerliste) auf die Schaltfläche "Add" (Hinzufügen).
2. Geben Sie im Feld "Username" (Benutzername) einen eindeutigen Namen ein (bis zu 16 Zeichen).
3. Geben Sie im Feld "Full Name" (Vollständiger Name) den vollständigen Namen des Benutzers ein (bis zu 64 Zeichen).
4. Geben Sie im Feld "Password" (Kennwort) ein Kennwort ein, und anschließend im Feld "Confirm Password" (Kennwort bestätigen) erneut (bis zu 64 Zeichen).
5. Wählen Sie in der Dropdown-Liste "User Group" (Benutzergruppe) die Gruppe aus.

   Wenn Sie diesen Benutzer keiner vorhandenen Benutzergruppe zuordnen möchten, wählen Sie in der Dropdownliste die Option "Individual Group" (Individuelle Gruppe) aus. Weitere Informationen zu den Berechtigungen einer individuellen Gruppe finden Sie unter ***Festlegen von Berechtigungen für eine individuelle Gruppe*** (auf Seite 116).
6. Lassen Sie das Kontrollkästchen "Active" (Aktiv) aktiviert, um den neuen Benutzer zu aktivieren. Klicken Sie auf "OK".

Ändern eines vorhandenen Benutzers

So ändern Sie einen vorhandenen Benutzer:

1. Öffnen Sie die Seite "User List" (Benutzerliste) unter "User Management" > "User List" (Benutzerverwaltung > Benutzerliste).



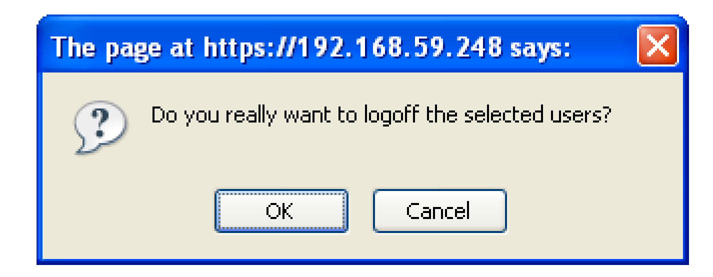
2. Wählen Sie den Benutzer aus der Liste auf der Seite "User List" (Benutzerliste) aus.
3. Klicken Sie auf den Benutzernamen. Die Seite "User" (Benutzer) wird angezeigt.
4. Bearbeiten Sie auf der Seite "User" (Benutzer) die entsprechenden Felder. Informationen zum Zugriff auf die Seite "User" (Benutzer) finden Sie unter ***Hinzufügen eines neuen Benutzers*** (auf Seite 118).
5. Klicken Sie auf "Delete" (Löschen), um einen Benutzer zu löschen. Sie werden aufgefordert, den Löschvorgang zu bestätigen.
6. Klicken Sie auf OK.

Abmelden eines Benutzers (Erzwungene Abmeldung)

Wenn Sie Administrator sind, können Sie andere lokal authentifizierte Benutzer, die auf LX angemeldet sind, abmelden.

So melden Sie einen Benutzer ab:

1. Öffnen Sie die Seite "User List" (Benutzerliste) unter "User Management" > "User List" (Benutzerverwaltung > Benutzerliste) oder klicken Sie auf den Link "Connected User" (Verbundene Benutzer) auf der linken Bildschirmseite.
2. Wählen Sie den Benutzer aus der Liste auf der Seite "User List" (Benutzerliste) aus und aktivieren Sie das Kontrollkästchen neben dem jeweiligen Benutzernamen.
3. Klicken Sie auf "Force User Logoff" (Benutzerabmeldung erzwingen).
4. Klicken Sie im Dialogfeld "Logoff User" (Benutzer abmelden) auf OK, um den Benutzer abzumelden.



5. Eine Bestätigungsmeldung über die erfolgreiche Benutzerabmeldung wird angezeigt. Diese Meldung enthält das Datum und die Uhrzeit der Abmeldung. Klicken Sie zum Schließen der Meldung auf OK.

Authentication Settings (Authentifizierungseinstellungen)

Bei der Authentifizierung geht es darum, die Identität des Benutzers zu überprüfen. Nach der Authentifizierung dient die Benutzergruppe dazu, die jeweiligen System- und Port-Berechtigungen zu ermitteln. Die dem Benutzer zugewiesenen Berechtigungen legen fest, welche Art des Zugriffs zulässig ist. Dies nennt man Autorisierung.

Wenn LX zur Remote-Authentifizierung konfiguriert ist, wird der externe Authentifizierungsserver hauptsächlich zur Authentifizierung verwendet und nicht zur Autorisierung.

Wenn Sie eine Schichtkonfiguration verwenden, in der ein LX-Basisgerät für den Zugriff auf mehrere andere Schichtgeräte verwendet wird, müssen das Basisgerät und die Schichtgeräte dieselben Authentifizierungseinstellungen verwenden.

Auf der Seite "Authentication Settings" (Authentifizierungseinstellungen) können Sie die Art der Authentifizierung für den Zugriff auf LX konfigurieren.

Hinweis: Wird der Benutzer bei aktivierter Remoteauthentifizierung (LDAP/LDAPS oder RADIUS) nicht gefunden, wird zusätzlich die Authentifizierungsdatenbank geprüft.

So konfigurieren Sie die Authentifizierung:

1. Wählen Sie "User Management > Authentication Settings" (Benutzerverwaltung > Authentifizierungseinstellungen). Die Seite "Authentication Settings" (Authentifizierungseinstellungen) wird angezeigt.
2. Wählen Sie die Option für das gewünschte Authentifizierungsprotokoll aus. Zur Verfügung stehen "Local Authentication" (Lokale Authentifizierung), "LDAP/LDAPS" oder "RADIUS". Bei Auswahl der Option "LDAP" werden die restlichen LDAP-Felder aktiviert, bei Auswahl der Option "RADIUS" die restlichen RADIUS-Felder.
3. Wenn Sie "Local Authentication" (Lokale Authentifizierung) auswählen, fahren Sie mit Schritt 6 fort.
4. Wenn Sie sich für "LDAP/LDAPS" entscheiden, lesen Sie den Abschnitt Implementierung der LDAP-Remoteauthentifizierung. Dort finden Sie Informationen zum Ausfüllen der Felder im Abschnitt "LDAP" der Seite "Authentication Settings" (Authentifizierungseinstellungen).
5. Wenn Sie sich für "RADIUS" entscheiden, lesen Sie den Abschnitt Implementierung der RADIUS-Remote-Authentifizierung. Dort finden Sie Informationen zum Ausfüllen der Felder im Bereich "RADIUS" der Seite "Authentication Settings" (Authentifizierungseinstellungen).



6. Klicken Sie zum Speichern auf "OK".

So stellen Sie die werksseitigen Standardeinstellungen wieder her:

- Klicken Sie auf "Reset to Defaults" (Standardeinstellungen wiederherstellen).

Implementierung der LDAP/LDAPS-Remoteauthentifizierung

Lightweight Directory Access Protocol (LDAP/LDAPS) ist ein Netzwerkprotokoll für die Abfrage und Änderung von Verzeichnisdiensten, die über TCP/IP ausgeführt werden. Ein Client startet eine LDAP-Sitzung, indem er eine Verbindung mit einem LDAP/LDAPS-Server herstellt (Standard-TCP-Port: 389). Anschließend sendet der Client Anfragen an den Server, und der Server sendet Antworten zurück.

Erinnerung: Microsoft Active Directory fungiert als LDAP/LDAPS-Authentifizierungsserver.

So verwenden Sie das LDAP-Authentifizierungsprotokoll:

1. Klicken Sie auf "User Management" > "Authentication Settings" (Benutzerverwaltung > Authentifizierungseinstellungen), um die Seite "Authentication Settings" (Authentifizierungseinstellungen) zu öffnen.
2. Wählen Sie das Optionsfeld "LDAP" aus, um den Abschnitt "LDAP" der Seite zu aktivieren.
3. Klicken Sie auf das ► LDAP-Symbol, um den Abschnitt "LDAP" zu erweitern.

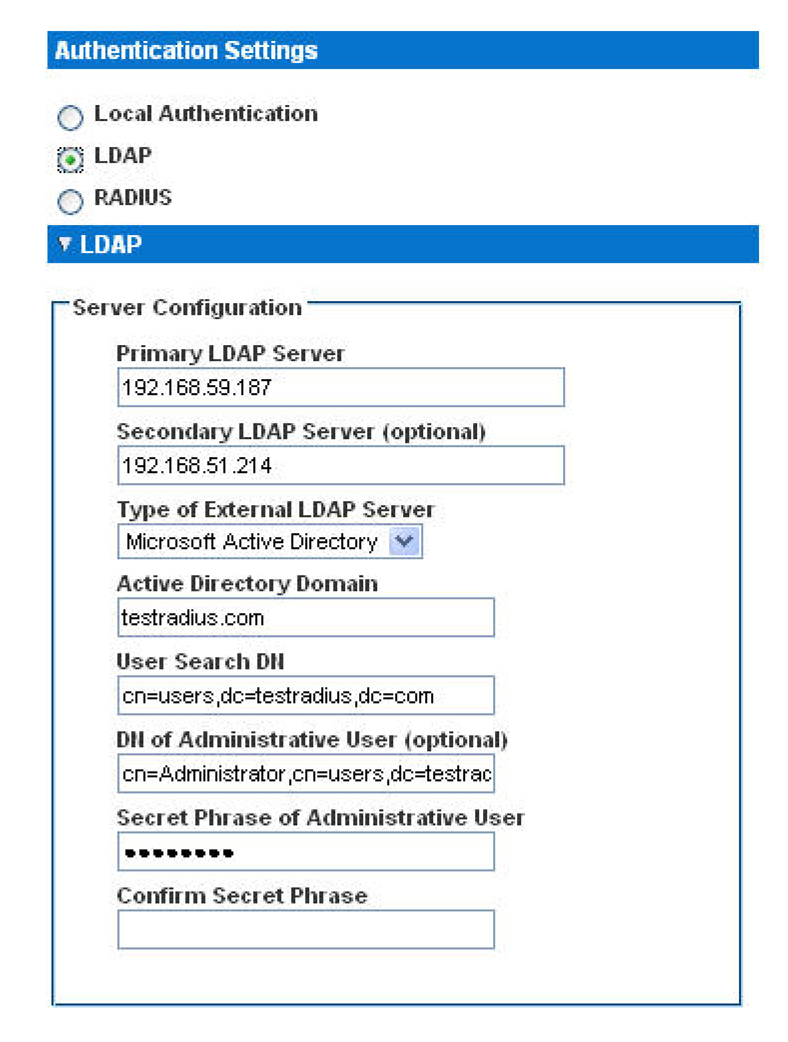
   Serverkonfiguration

4. Geben Sie im Feld "Primary LDAP Server" (Primärer LDAP-Server) die IP-Adresse oder den DNS-Namen des LDAP/LDAPS-Remote-Authentifizierungsservers ein (bis zu 256 Zeichen). Sind die Optionen "Enable Secure LDAP" (Secure LDAP aktivieren) und "Enable LDAPS Server Certificate Validation" (LDAPS-Serverzertifikat-Validierung aktivieren) ausgewählt, muss der DNS-Name verwendet werden, um dem CN des LDAP-Serverzertifikats zu entsprechen.
5. Geben Sie im Feld "Secondary LDAP Server" (Sekundärer LDAP-Server) die IP-Adresse oder den DNS-Namen des LDAP/LDAPS-Sicherungsservers ein (bis zu 256 Zeichen). Wenn die Option "Enable Secure LDAP" (Secure LDAP aktivieren) ausgewählt ist, muss der DNS-Name verwendet werden. Für die restlichen Felder gelten die gleichen Einstellungen wie für "Primary LDAP Server" (Primärer LDAP-Server). **Optional**
6. "Type of external LDAP Server" (Typ des externen LDAP-Servers)

7. Wählen Sie den externen LDAP/LDAPS-Server aus. Wählen Sie eine der folgenden Optionen:
   - "Generic LDAP Server" (Generischer LDAP-Server)
   - Microsoft Active Directory. Microsoft hat die LDAP/LDAPS-Verzeichnisdienste in Active Directory für die Verwendung in Windows-Umgebungen implementiert.
8. Geben Sie den Namen der Active Directory-Domäne ein, wenn Sie Microsoft Active Directory ausgewählt haben. Zum Beispiel *acme.com*. Fragen Sie Ihren leitenden Administrator nach einem speziellen Dömanennamen.
9. Geben Sie in das Feld "User Search DN" (DN für Benutzersuche) den Distinguished Name ein, bei dem Sie die Suche nach Benutzerinformationen in der LDAP-Datenbank beginnen möchten. Es können bis zu 64 Zeichen verwendet werden. Ein Beispiel für einen Basissuchwert ist: `cn=Benutzer,dc=raritan,dc=com`. Fragen Sie den Administrator des Authentifizierungsservers nach den korrekten Werten für diese Felder.
10. Geben Sie den Distinguished Name (DN) des Administratorbenutzers in das Feld "DN of Administrative User" (DN des Administratorbenutzers) ein (maximal 64 Zeichen). Füllen Sie dieses Feld aus, wenn Ihr LDAP-Server nur Administratoren die Suche nach Benutzerinformationen mithilfe der Funktion "Administrative User" (Administratorbenutzer) gestattet. Fragen Sie den Administrator des Authentifizierungsservers nach den korrekten Werten für dieses Feld. Ein Wert für "DN of administrative User" (DN des Administratorbenutzers) könnte wie folgt aussehen: `cn=Administrator,cn=Benutzer,dc=testradius,dc=com`. **Optional**



11. Wenn Sie einen "Distinguished Name" (DN) für den Administratorbenutzer eingeben, müssen Sie das Kennwort eingeben, um den DN des Administratorbenutzers am Remote-Authentifizierungsserver zu authentifizieren. Geben Sie das Kennwort in das Feld "Secret Phrase" (Geheimer Schlüssel) und ein weiteres Mal in das Feld "Confirm Secret Phrase" (Geheimen Schlüssel bestätigen) ein (maximal 128 Zeichen).



LDAP/LDAP Secure

12. Aktivieren Sie das Kontrollkästchen "Enable Secure LDA" (Secure LDAP aktivieren), wenn Sie SSL verwenden möchten. Dadurch wird das Kontrollkästchen "Enable LDAPS Server Certificate Validation" (LDAPS-Serverzertifikat-Validierung aktivieren) aktiviert. Secure Sockets Layer (SSL) ist ein kryptografisches Protokoll, über das LX sicher mit dem LDAP/LDAPS-Server kommunizieren kann.

13. Der Standardport lautet 389. Verwenden Sie entweder den Standard-TCP-Port für LDAP oder legen Sie einen anderen Port fest.



14. Der standardmäßige Secure LDAP-Port lautet 636. Verwenden Sie entweder den Standardport oder legen Sie einen anderen Port fest. Dieses Feld wird nur verwendet, wenn das Kontrollkästchen "Enable Secure LDAP" (Secure LDAP aktivieren) aktiviert ist.
15. Aktivieren Sie das Kontrollkästchen "Enable LDAPS Server Certificate Validation" (LDAPS-Serverzertifikat-Validierung aktivieren), und verwenden Sie die zuvor hochgeladene CA-Stammzertifikatdatei zur Validierung des vom Server bereitgestellten Zertifikats. Wenn Sie die zuvor hochgeladene CA-Stammzertifikatdatei nicht verwenden möchten, lassen Sie das Kontrollkästchen deaktiviert. Die Deaktivierung dieser Funktion entspricht der Annahme des Zertifikats einer unbekannten Zertifizierungsstelle. Dieses Kontrollkästchen ist nur verfügbar, wenn das Kontrollkästchen "Enable Secure LDAP" (Secure LDAP aktivieren) aktiviert wurde.

Hinweis: Ist zusätzlich zur CA-Stammzertifikat-Validierung die Option "Enable LDAPS Server Certificate Validation" (LDAPS-Serverzertifikat-Validierung aktivieren) aktiviert, muss der Hostname des Servers mit dem bereitgestellten allgemeinen Namen im Serverzertifikat übereinstimmen.

---

16. Laden Sie die CA-Stammzertifikatdatei hoch, falls dies erforderlich ist. Dieses Feld steht zur Verfügung, wenn das Kontrollkästchen "Enable Secure LDAP" (Secure LDAP aktivieren) aktiviert ist. Fragen Sie den Administrator des Authentifizierungsservers nach der CA-Zertifikatdatei im Base64-codierten X-509-Format für den LDAP-/LDAPS-Server. Navigieren Sie über die Schaltfläche "Browse" (Durchsuchen) zur entsprechenden Zertifikatdatei. Wenn Sie ein Zertifikat für den LDAP-/LDAPS-Server durch ein neues Zertifikat ersetzen, müssen Sie LX neu starten, damit das neue Zertifikat wirksam wird.

LDAP / Secure LDAP
Enable Secure LDAP
Port
389
Secure LDAP Port
636
Enable LDAPS Server Certificate Validation
Root CA Certificate File
Browse...
Upload
Note: Reboot device after certificate file is uploaded.

Testen des LDAP-Serverzugriffs

17. LX bietet Ihnen aufgrund der Komplexität einer erfolgreichen Konfigurierung von LDAP-Server und LX zur Remoteauthentifizierung die Möglichkeit, die LDAP-Konfigurierung auf der Seite "Authentication Settings" (Authentifizierungseinstellungen) zu testen. Um die Authentifizierungseinstellungen zu testen, geben Sie den Anmeldenamen in das das Feld "Login for testing" (Anmeldung für Test) und das Kennwort in das Feld "Password for testing" (Kennwort für Test) ein. Das sind der Benutzername und das Kennwort, die Sie für den Zugriff auf LX eingegeben haben und die vom LDAP-Server für Ihre Authentifizierung verwendet werden. Klicken Sie auf "Test".

    Ist der Test abgeschlossen, wird Ihnen in einer Meldung angezeigt, ob der Test erfolgreich war oder nicht. Ist der Test fehlgeschlagen, wird Ihnen eine detaillierte Fehlermeldung angezeigt. Es wird das Ergebnis des erfolgreich durchgeführten Tests oder, falls der Test nicht erfolgreich war, eine detaillierte Fehlermeldung angezeigt. Außerdem können Gruppeninformationen angezeigt werden, die im Falle eines erfolgreichen Tests für den Testbenutzer vom LDAP-Remoteserver abgerufen werden.

Test LDAP Server Access

Login for testing

Password for testing

Test

Rückgabe von Benutzergruppeninformationen vom Active Directory-Server

LX unterstützt die Benutzerauthentifizierung zu Active Directory® (AD), ohne dass Benutzer lokal in LX definiert sein müssen. Dadurch können Active Directory-Benutzerkonten und -Kennwörter ausschließlich auf dem Active Directory-Server verwaltet werden. Die Autorisierungs- und Active Directory-Benutzerrechte werden mit standardmäßigen LX-Richtlinien und Benutzergruppenrechten, die lokal auf Active Directory-Benutzergruppen angewendet werden, gesteuert und verwaltet.

WICHTIG: Wenn Sie bereits Kunde von Raritan, Inc. sind und den Active Directory-Server bereits durch Ändern des Active Directory-Schemas konfiguriert haben, unterstützt LX diese Konfiguration nach wie vor, und Sie müssen den folgenden Vorgang nicht durchführen. Informationen zur Aktualisierung des Active

Directory-LDAP/LDAPS-Schemas finden Sie unter *Aktualisieren des LDAP-Schemas* (auf Seite 241).

So aktivieren Sie den AD-Server auf der LX-Einheit:

1. Erstellen Sie auf der LX-Einheit besondere Gruppen und weisen Sie ihnen geeignete Berechtigungen zu. Erstellen Sie z. B. Gruppen wie "KVM_Admin" und "KVM_Operator".
2. Erstellen Sie auf dem Active Directory-Server neue Gruppen mit denselben Gruppennamen wie die im vorherigen Schritt erstellten Gruppen.
3. Weisen Sie die LX-Benutzer auf dem AD-Server den Gruppen zu, die Sie in Schritt 2 erstellt haben.
4. Aktivieren und konfigurieren Sie den AD-Server auf der LX-Einheit. Siehe ***Implementierung der LDAP/LDAPS-Remoteauthentifizierung*** (auf Seite 121).

Wichtige Hinweise:

- Bei der Eingabe des Gruppennamens muss die Groß-/Kleinschreibung beachtet werden.
- LX bietet folgende Standardgruppen, die nicht geändert oder gelöscht werden können: "Admin" und "<Unknown>" (Unbekannt). Stellen Sie sicher, dass diese Gruppennamen nicht auch vom Active Directory-Server verwendet werden.
- Wenn die vom Active Directory-Server zurückgegebenen Gruppeninformationen nicht mit der LX-Gruppenkonfiguration übereinstimmen, weist LX den Benutzern, die sich erfolgreich authentifizieren, automatisch die Gruppe "<Unknown>" (Unbekannt) zu.
- Wenn Sie eine Rückrufnummer verwenden, müssen Sie die folgende Zeichenfolge unter Beachtung der Groß-/Kleinschreibung eingeben: *msRADIUSCallbackNumber.*
- Auf Empfehlung von Microsoft sollten "Global Groups" (globale Gruppen) mit Benutzerkonten verwendet werden, keine "Domain Local Groups" (lokale Domaingruppen).



Implementierung der RADIUS-Remote-Authentifizierung

Remote Authentication Dial-in User Service (RADIUS) ist ein AAA-Protokoll [Authentication, Authorization Accounting (Authentifizierung, Autorisierung und Kontoführung)] für Anwendungen für den Netzwerkzugriff.

So verwenden Sie das RADIUS-Authentifizierungsprotokoll:

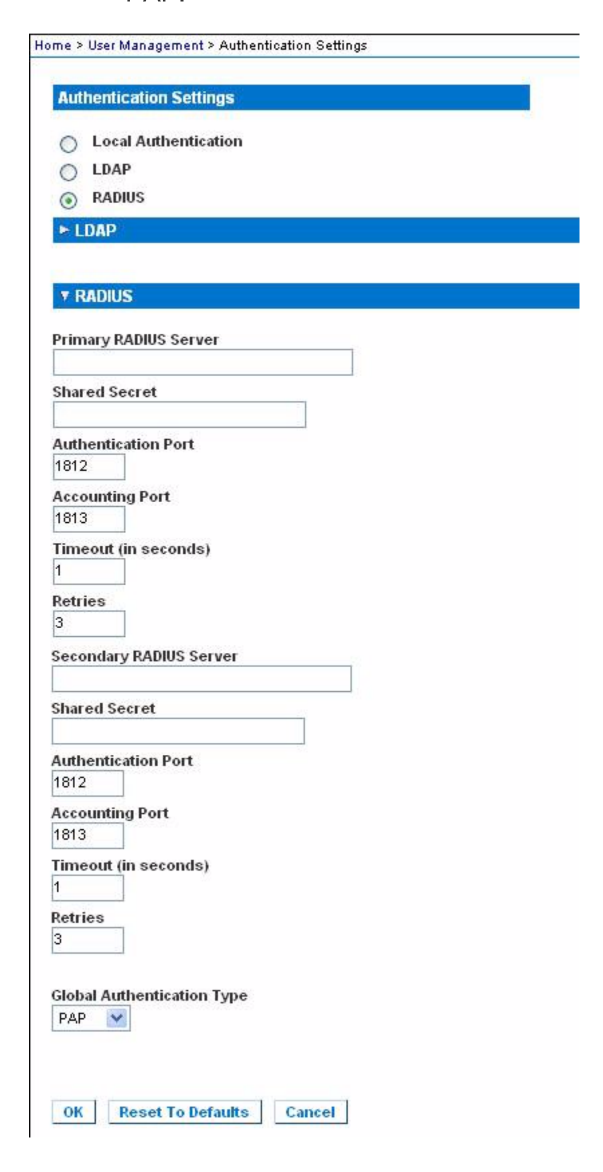
1. Klicken Sie auf "User Management" > "Authentication Settings" (Benutzerverwaltung > Authentifizierungseinstellungen), um die Seite "Authentication Settings" (Authentifizierungseinstellungen) zu öffnen.
2. Klicken Sie auf das Optionsfeld "RADIUS", um den Abschnitt "RADIUS" der Seite zu aktivieren.
3. Klicken Sie auf das RADIUS-Symbol, um den Abschnitt "RADIUS" zu erweitern.
4. Geben Sie in den Feldern "Primary Radius Server" (Primärer RADIUS-Server) und "Secondary Radius Server" (Sekundärer RADIUS-Server) die jeweiligen IP-Adressen des primären und optionalen sekundären Remote-Authentifizierungsservers ein (bis zu 256 Zeichen).
5. Geben Sie im Feld "Shared Secret" (Gemeinsamer geheimer Schlüssel) den geheimen Schlüssel für die Authentifizierung ein (bis zu 128 Zeichen).

   Der gemeinsame geheime Schlüssel ist eine Zeichenfolge, die LX und dem RADIUS-Server bekannt sein muss, damit diese sicher kommunizieren können. Es handelt sich dabei praktisch um ein Kennwort.
6. Der Standardport für "Authentication Port" (Authentifizierungsport) lautet 1812, kann jedoch nach Bedarf geändert werden.
7. Der Standardport für "Accounting Port" (Kontoführungsport) lautet 1813, kann jedoch nach Bedarf geändert werden.
8. Das "Timeout" (Zeitlimit) wird in Sekunden aufgezeichnet. Der Standardwert beträgt 1 Sekunde, kann jedoch bei Bedarf geändert werden.

   Das Zeitlimit bezeichnet die Zeitspanne, während der LX auf eine Antwort vom RADIUS-Server wartet, ehe eine weitere Authentifizierungsanforderung gesendet wird.
9. Die standardmäßige Anzahl an Neuversuchen beträgt 3.

   Dieser Wert gibt an, wie oft LX eine Authentifizierungsanforderung an den RADIUS-Server sendet.
10. Wählen Sie in der Dropdownliste den "Global Authentication Type" (Globaler Authentfizierungstyp) aus:

- PAP – Mit PAP werden Kennwörter als unformatierter Text gesendet. PAP ist nicht interaktiv. Benutzername und Kennwort werden als ein Datenpaket gesendet, sobald eine Verbindung hergestellt wurde. Der Server sendet nicht zuerst eine Anmeldeaufforderung und wartet auf eine Antwort.
- CHAP – Mit CHAP kann der Server jederzeit eine Authentifizierung anfordern. CHAP bietet mehr Sicherheit als PAP.





Cisco ACS 5.x für RADIUS-Authentifizierung

Bei Verwendung eines Cisco ACS 5.x Servers führen Sie nach dem Konfigurieren von LX für die RADIUS-Authentifizierung die folgenden Schritte auf dem Cisco ACS 5.x Server aus.

Hinweis: Die folgenden Schritte umfassen die Cisco Menüs und Menüelemente, die für den Zugriff auf die einzelnen Seiten verwendet werden. Aktuelle Informationen und weitere Einzelheiten zum Ausführen der einzelnen Schritte finden Sie in der Cisco Dokumentation.

- LX als AAA-Client hinzufügen (**Erforderlich**) – "Network Resources" (Netzwerkressourcen) > "Network Device Group" (Netzwerkgeräte-Gruppe)> "Network Device and AAA Clients" (Netzwerkgerät und AAA-Clients)
- Benutzer hinzufügen/bearbeiten (**Erforderlich**) – "Network Resources" (Netzwerkressourcen) > "Users and Identity Stores" (Benutzer und Identitätsspeicher) > "Internal Identity Stores" (Interne Identitätsspeicher) > "Users" (Benutzer)
- Standardnetzwerkzugriff zur Aktivierung des CHAP-Protokolls konfigurieren (**Optional**) – "Policies" (Richtlinien) > "Access Services" (Zugriffsdienste) > "Default Network Access" (Standardnetzwerkzugriff)
- Autorisierungsregeln zur Zugriffskontrolle erstellen (**Erforderlich**) – "Policy Elements" (Richtlinienelemente) > "Authorization and Permissions" (Autorisierung und Berechtigungen) > "Network Access" (Netzwerkzugriff) > "Authorization Profiles" (Autorisierungsprofile)
  - Wörterbuchtyp: RADIUS-IETF
  - RADIUS-Attribut: Filter-ID
  - Attributtyp: Zeichenfolge
  - Attributwert: Raritan:G{KVM_Admin} (wobei KVM_Admin der Gruppenname ist, der lokal auf dem Dominion KVM-Switch erstellt wird). Die Groß-/Kleinschreibung muss beachtet werden.
- Sitzungsbedingungen konfigurieren (Datum und Uhrzeit) (**Erforderlich**) – "Policy Elements" (Richtlinienelemente) > "Session Conditions" (Sitzungsbedingungen) > "Date and Time" (Datum und Uhrzeit)
- Die Autorisierungsrichtlinie für den Netzwerkzugriff konfigurieren/erstellen (**Erforderlich**) – "Access Policies" (Zugriffsrichtlinien) > "Access Services" (Zugriffsdienste) > "Default Network Access" (Standardnetzwerkzugriff) > "Authorization" (Autorisierung)

Zurückgeben von Benutzergruppeninformationen über RADIUS

Wenn ein RADIUS-Authentifizierungsversuch erfolgreich ist, bestimmt LX die Berechtigungen eines Benutzers anhand der Berechtigungen der Gruppe des Benutzers.

Ihr Remote-RADIUS-Server kann diese Benutzergruppennamen bereitstellen, indem er ein als RADIUS FILTER-ID implementiertes Attribut zurückgibt. Die FILTER-ID sollte folgendermaßen formatiert sein: Raritan:G{*GROUP_NAME*}. Dabei ist *GROUP_NAME* eine Zeichenfolge, die den Namen der Gruppe angibt, der der Benutzer angehört.

```
Raritan:G{GROUP_NAME}:D{Dial Back Number}
```

Dabei ist "GROUP_NAME" eine Zeichenfolge, die den Namen der Gruppe angibt, der der Benutzer angehört, und "Dial Back Number" die dem Benutzerkonto zugeordnete Nummer, die das LX-Modem für den Rückruf des Benutzerkontos verwendet.

Spezifikationen für den RADIUS-Kommunikationsaustausch

LX sendet die folgenden RADIUS-Attribute an Ihren RADIUS-Server:

Attribut	Daten
Anmelden	
Access-Request (1)	
NAS-Port-Type (61)	VIRTUAL (5) für Netzwerkverbindungen.
NAS-IP-Address (4)	Die IP-Adresse des LX.
User-Name (1)	Dies ist der in der Anmeldemaske eingegebene Benutzername.
Acct-Session-ID (44)	Sitzungs-ID für Kontoführung.
User-Password(2)	Das verschlüsselte Kennwort.
Accounting-Request(4)	
Acct-Status (40)	Start(1) – Kontoführung wird gestartet.
NAS-Port-Type (61)	VIRTUAL (5) für Netzwerkverbindungen.
NAS-Port (5)	Dieses Attribut ist immer 0.
NAS-IP-Address (4)	Die IP-Adresse des LX.
User-Name (1)	Dies ist der in der Anmeldemaske eingegebene Benutzername.
Acct-Session-ID (44)	Sitzungs-ID für Kontoführung.



Attribut	Daten
Abmelden	
Accounting-Request(4)	
Acct-Status (40)	Stop(2) – Kontoführung wird beendet.
NAS-Port-Type (61)	VIRTUAL (5) für Netzwerkverbindungen.
NAS-Port (5)	Dieses Attribut ist immer 0.
NAS-IP-Address (4)	Die IP-Adresse des LX.
User-Name (1)	Dies ist der in der Anmeldemaske eingegebene Benutzername.
Acct-Session-ID (44)	Sitzungs-ID für Kontoführung.

Benutzerauthentifizierungsprozess

Die Remoteauthentifizierung wird über den im folgenden Diagramm angegebenen Vorgang durchgeführt:

User logs in

Is Remote Authentication Enabled?

No

Yes

Is Remote Authentication Server reachable?

No

No

Yes

Is User authenticated in local database?

Is User authenticated in remote database?

Yes

Yes

User allowed

No

User denied

Ändern von Kennwörtern

So ändern Sie Ihr Kennwort:

1. Wählen Sie "User Management" > "Change Password" (Benutzerverwaltung > Kennwort ändern). Die Seite "Change Password" (Kennwort ändern) wird angezeigt.
2. Geben Sie im Feld "Old Password" (Altes Kennwort) Ihr aktuelles Kennwort ein.
3. Geben Sie in das Feld "New Password" (Neues Kennwort) ein neues Kennwort ein. Geben Sie das Kennwort im Feld "Confirm New Password" (Neues Kennwort bestätigen) erneut ein. Ein Kennwort kann aus bis zu 64 alphanumerischen Zeichen der englischen Sprache sowie Sonderzeichen bestehen.
4. Klicken Sie auf OK.
5. Die erfolgreiche Änderung des Kennworts wird bestätigt. Klicken Sie auf OK.

Hinweis: Wenn sichere Kennwörter verwendet werden müssen, enthält diese Seite Informationen zum erforderlichen Format. Weitere Informationen zu Kennwörtern und sicheren Kennwörtern finden Sie unter **Sichere Kennwörter** *(siehe "***Strong Passwords (Sichere Kennwörter)***" auf Seite 165).*

Home > User Management > Change Password

Change Password

Old Password

New Password

Confirm New Password

OK Cancel

Kapitel 6 Geräteverwaltung

In diesem Kapitel

Network Settings (Netzwerkeinstellungen)

Auf der Seite "Network Settings" (Netzwerkeinstellungen) können Sie die Netzwerkkonfiguration (z. B. IP-Adresse, Erkennungsport und LAN-Schnittstellenparameter) für Ihre LX-Einheit anpassen.

Es stehen Ihnen zwei Optionen zum Festlegen der IP-Konfiguration zur Verfügung:

- None (default) [Keine (Standard)] – Dies ist die empfohlene Option (statisches IP). Da die LX-Einheit Teil Ihrer Netzwerkinfrastruktur ist, möchten Sie wahrscheinlich, dass die Adresse möglichst konstant bleibt. Bei dieser Option können Sie die Netzwerkparameter selbst einrichten.
- DHCP – Mit dieser Option wird die IP-Adresse automatisch durch einen DHCP-Server zugewiesen.

So ändern Sie die Netzwerkkonfiguration:

1. Wählen Sie "Device Settings" > "Network" (Geräteeinstellungen > Netzwerk) aus. Die Seite "Network Settings" (Netzwerkeinstellungen) wird angezeigt.
2. Aktualisieren der Basisnetzwerkeinstellungen. Siehe ***Basisnetzwerkeinstellungen*** (auf Seite 135).
3. Aktualisieren der LAN-Schnittstelleneinstellungen. Siehe LAN-Schnittstelleneinstellungen.
4. Klicken Sie auf OK, um die Konfiguration festzulegen. Ist für die vorgenommenen Änderungen ein Neustart des Geräts erforderlich, wird eine entsprechende Meldung angezeigt.

So kehren Sie zu den Werkseinstellungen zurück:

- Klicken Sie auf "Reset to Defaults" (Standardeinstellungen wiederherstellen).

Basisnetzwerkeinstellungen

Im Folgenden wird das Zuweisen einer IP-Adresse auf der Seite "Network Settings" (Netzwerkeinstellungen) beschrieben. Umfassende Informationen zu allen Feldern sowie zur Funktionsweise dieser Seite finden Sie unter ***Netzwerkeinstellungen*** (siehe "***Network Settings (Netzwerkeinstellungen)***" auf Seite 134).

So weisen Sie eine IP-Adresse zu:

1. Wählen Sie "Device Settings > Network" (Geräteeinstellungen > Netzwerk). Die Seite "Network Settings" (Netzwerkeinstellungen) wird angezeigt.
2. Geben Sie einen aussagekräftigen Namen für Ihr LX-Gerät an. Verwenden Sie dazu bis zu 32 gültige Sonderzeichen und keine Leerzeichen.
3. Geben Sie im Bereich "IPv4" die entsprechenden IPv4-spezifischen Netzwerkeinstellungen ein oder wählen Sie diese aus:
   a. Geben Sie eine IP-Adresse ein, falls erforderlich. Die Standard-IP-Adresse lautet 192.168.0.192.
   b. Geben Sie die Subnetzmaske ein. Die Standardsubnetzmaske lautet 255.255.255.0.
   c. Geben Sie das Standardgateway ein, wenn in der Dropdownliste unter "IP Auto Configuration" (Automatische IP-Konfiguration) "None" (Keine) ausgewählt ist.
   d. Geben Sie den Namen des bevorzugten DHCP-Hosts ein, wenn in der Dropdownliste unter "IP Auto Configuration" (Automatische IP-Konfiguration) "DHCP" ausgewählt ist.
   e. Wählen Sie "IP Auto Configuration" (Automatische IP-Konfiguration) aus. Folgende Optionen stehen zur Verfügung:

   - None (Static IP) [Keine (Statisches IP)] – Bei Auswahl dieser Option müssen Sie die Netzwerkparameter manuell angeben.

     Diese Option wird empfohlen, da LX ein Infrastrukturgerät ist, dessen IP-Adresse sich nicht ändern sollte.

   - DHCP – Dynamic Host Configuration Protocol wird von Netzwerkcomputern (Clients) verwendet, um eindeutige IP-Adressen und andere Parameter von einem DHCP-Server zu erhalten.

     Bei Auswahl dieser Option werden die Netzwerkparameter vom DHCP-Server zugewiesen. Bei Verwendung von DHCP geben Sie unter "Preferred host name (DHCP only)" (Name des bevorzugten Hosts [Nur DHCP]) einen Wert ein (maximal 63 Zeichen).



4. Wenn IPv6 verwendet werden soll, geben Sie im Bereich "IPv6" die entsprechenden IPv6-spezifischen Netzwerkeinstellungen ein oder wählen Sie diese aus:
   a. Aktivieren Sie das Kontrollkästchen "IPv6", um die Felder in diesem Bereich zu aktivieren.
   b. Geben Sie eine globale/eindeutige IP-Adresse ein. Dies ist die IP-Adresse, die dem LX zugeordnet ist.
   c. Geben Sie die Präfixlänge ein. Dies ist die Anzahl der Bits, die in der IPv6-Adresse verwendet werden.
   d. Geben Sie die IP-Adresse des Gateway ein.
   e. Link-Local-IP-Adresse. Diese Adresse wird dem Gerät automatisch zugewiesen. Sie wird zum Erkennen von Nachbarn verwendet oder wenn keine Router verfügbar sind. **Read-Only (Lese-zugriff)**
   f. Zonen-ID. Hierdurch wird das Gerät identifiziert, dem die Adresse zugeordnet ist. **Read-Only (Lese-zugriff)**
   g. Wählen Sie "IP Auto Configuration" (Automatische IP-Konfiguration) aus. Folgende Optionen stehen zur Verfügung:
   - None (Keine) – Wählen Sie diese Option aus, wenn Sie keine automatische IP-Konfiguration wünschen, sondern die IP-Adresse lieber selbst festlegen (statisches IP). Diese Option ist voreingestellt und wird empfohlen.

     Wenn für "IP auto configuration" (Automatische IP-Konfiguration) "None" (Keine) ausgewählt ist, sind die folgenden "Network Basic Settings" (Basisnetzwerkeinstellungen) aktiviert: "Global/Unique IP Address" (Globale/Eindeutige IP-Adresse), "Prefix Length" (Präfixlange) und "Gateway IP Address" (Gateway-IP-Adresse) ermöglichen Ihnen die manuelle IP-Konfiguration.
   - Router Discovery (Router-Erkennung) – Verwenden Sie diese Option, um IPv6-Adressen, deren Signifikanz "Global" oder "Unique Local" (Lokal eindeutig) ist und über der von Link Local liegt, welche nur für ein direkt verbundenes Subnetz gültig ist, automatisch zuzuordnen.
5. Wenn DHCP ausgewählt ist, wählen Sie "Obtain DNS Server Address Automatically" (DNS-Serveradresse automatisch abrufen) aus, um diese Funktion zu aktivieren. Wenn die DNS-Serveradresse automatisch abgerufen wird, werden die vom DHCP-Server bereitgestellten DNS-Informationen verwendet.
6. Wenn "Use the Following DNS Server Addresses" (Die folgenden DNS-Serveradressen verwenden) ausgewählt ist, werden die in diesem Abschnitt eingegebenen Adressen für die Verbindung zum DNS-Server verwendet, unabhängig davon, ob DHCP ausgewählt wurde.



Geben Sie die folgenden Informationen ein, wenn die Option "Following DNS Server Addresses" (Folgende DNS-Serveradressen) ausgewählt wurde. Diese Adressen sind die primären und sekundären DNS-Adressen, die verwendet werden, wenn die primäre DNS-Serververbindung aufgrund eines Ausfalls getrennt wird.

a. Primary DNS Server IP Address (IP-Adresse des primären DNS-Servers)

b. Secondary DNS-Server IP Address (IP-Adresse des sekundären DNS-Servers)

7. Klicken Sie abschließend auf OK.

Weitere Informationen zur Konfiguration dieses Bereichs der Seite "Network Settings" (Netzwerkeinstellungen) finden Sie unter LAN-Schnittstelleneinstellungen.

Hinweis: Bei manchen Umgebungen gibt die Standardeinstellung "Autodetect" (automatische Aushandlung) für "LAN Interface Speed & Duplex" (LAN-Schnittstellengeschwindigkeit und Duplex) die Netzwerkparameter nicht richtig vor, was zu Netzwerkproblemen führen kann. Wählen Sie in einem solchen Fall im Feld "LAN Interface Speed & Duplex" des LX den Wert "100 Mbps/Full Duplex" (100 Mbit/s/Vollduplex) (bzw. die geeignete Option für Ihr Netzwerk) aus, um dieses Problem zu beheben.Weitere Informationen finden Sie auf der Seite **Network Settings** *(siehe "***Network Settings (Netzwerkeinstellungen)***" auf Seite 134) (Netzwerkeinstellungen).*

Basic Network Settings
Device Name *
se-lx2-232
IPv4 Address
IP Address
192.168.51.55
Subnet Mask
255.255.255.0
Default Gateway
192.168.51.126
Preferred DHCP Host Name
IP Auto Configuration
DHCP
IPv6 Address
Global/Unique IP Address
Prefix Length
Gateway IP Address
Link-Local IP Address
Zone ID
N/A
%1
IP Auto Configuration
None
Obtain DNS Server Address Automatically
Use the Following DNS Server Addresses
Primary DNS Server IP Address
192.168.59.2
Secondary DNS Server IP Address
192.168.51.10
OK
Reset To Defaults
Cancel



"LAN Interface Settings" (LAN-Schnittstelleneinstellungen)

Die aktuellen Parametereinstellungen werden im Feld "Current LAN interface parameters" (Aktuelle LAN-Schnittstellenparameter) angezeigt.

1. Wählen Sie "Device Settings > Network" (Geräteeinstellungen > Netzwerk). Die Seite "Network Settings" (Netzwerkeinstellungen) wird angezeigt.
2. Wählen Sie aus folgenden Optionen die LAN-Schnittstellengeschwindigkeit & Duplex aus:
   - "Autodetect (default option)" [Automatische Aushandlung (Standardoption)]
   - "10 Mbps/Half" (10 Mbit/s/Halb – Beide LEDs blinken)
   - "10 Mbps/Full" (10 Mbit/s/Voll) – Beide LEDs blinken
   - "100 Mbps/Half" (100 Mbit/s/Halb) – Gelbe LED blinkt
   - "100 Mbps/Full" (100 Mbit/s/Voll) – Gelbe LED blinkt
   - "1000 Mbps/Full (gigabit)" (1000 Mbit/s/Voll (Gigabit)) – grüne LED blinkt
   - "Half-duplex" (Halbduplex) sorgt für Kommunikation in beide Richtungen, jedoch nicht gleichzeitig.
   - "Full-duplex" (Vollduplex) ermöglicht die gleichzeitige Kommunikation in beide Richtungen.

   Hinweis: Bei 10 Mbit/s und Halb- oder Vollduplex kann es gelegentlich zu Problemen kommen. Verwenden Sie in einem solchen Fall eine andere Geschwindigkeit und Duplexeinstellung.

   Weitere Informationen finden Sie unter ***Netzwerk-Geschwindigkeitseinstellungen*** (auf Seite 239).
3. Wählen Sie die Bandbreite aus.
4. Klicken Sie auf "OK", um die LAN-Einstellungen zu übernehmen.

"Device Services" (Gerätedienste)

Auf der Seite "Device Services" (Gerätedienste) können Sie die folgenden Funktionen konfigurieren:

- SSH-Zugriff aktivieren
- Schichten für das Basis-LX aktivieren
- Erkennungsport eingeben
- Direkten Portzugriff aktivieren
- AKC-Download-Serverzertifikat-Validierung aktivieren, falls Sie AKC verwenden

Aktivieren von SSH

Wählen Sie "Enable SSH Access" (SSH-Zugriff aktivieren) aus, damit Administratoren über die SSH v2-Anwendung auf LX zugreifen können.

So aktivieren Sie den SSH-Zugriff:

1. Wählen Sie "Device Settings > Device Services" (Geräteeinstellungen > Gerätedienste). Die Seite "Device Service Settings" (Gerätediensteinstellungen) wird geöffnet.
2. Wählen Sie "Enable SSH Access" (SSH-Zugriff aktivieren) aus.
3. Geben Sie die SSH-Portinformationen ein. Die standardmäßige SSH-TCP-Portnummer lautet 22, sie kann jedoch geändert werden, um ein höheres Niveau für Sicherheitsvorgänge zu erreichen.
4. Klicken Sie auf OK.

HTTP- und HTTPS-Porteinstellungen

Sie können von LX verwendete HTTP- und/oder HTTPS-Ports konfigurieren. Wenn Sie z. B. den Standard-HTTP-Port 80 für andere Zwecke nutzen, wird beim Ändern des Ports sichergestellt, dass das Gerät nicht versucht, diesen Port zu verwenden.

So ändern Sie die HTTP- und/oder HTTPS-Porteinstellungen:

1. Wählen Sie "Device Settings > Device Services" (Geräteeinstellungen > Gerätedienste). Die Seite "Device Service Settings" (Gerätediensteinstellungen) wird geöffnet.
2. Geben Sie die neuen Ports in die Felder "HTTP Port" und/oder "HTTPS Port" ein.
3. Klicken Sie auf OK.

Eingeben des Erkennungsports

Die LX-Erkennung erfolgt über einen einzelnen konfigurierbaren TCP-Port. Der Standardport lautet 5000, Sie können diesen jedoch für die Verwendung aller TCP-Ports außer 80 und 443 konfigurieren. Wenn Sie über eine Firewall auf LX zugreifen möchten, müssen die Firewalleinstellungen die ein- und ausgehende Kommunikation über den Standardport 5000 bzw. den nicht-standardmäßigen konfigurierten Port zulassen.

So aktivieren Sie den Erkennungsport:

1. Wählen Sie "Device Settings > Device Services" (Geräteeinstellungen > Gerätedienste). Die Seite "Device Service Settings" (Gerätediensteinstellungen) wird geöffnet.



2. Geben Sie unter "Discovery Port" (Erkennungsport) den Erkennungsport ein.
3. Klicken Sie auf OK.



Konfigurieren und Aktivieren von Schichten

LX und generische Schichtfunktionen werden von LX unterstützt. Mit der Schichtfunktion können Sie über ein >ProductName<-Basisgerät auf LX-Ziele zugreifen.

Hinweis: Für Basis- und Schichtgeräte muss dieselbe Firmware-Version verwendet werden.

Sie können bei Bedarf maximal zwei Schichtebenen an Geräten zu einer Konfiguration hinzufügen oder aus einer Konfiguration löschen.

Beim Einrichten der Geräte verwenden Sie spezifische CIMS für spezifische Konfigurationen. Eine Beschreibung der Ziele, die Sie in eine Schichtkonfiguration einfügen können, sowie Informationen zur CIM-Kompatibilität und Gerätekonfiguration finden Sie unter ***Schichten – Zieltypen, unterstützte CIMs und Schichtkonfiguration*** (siehe "***Schichten – Zieltypen, unterstützte CIMs und Schichtkonfigurationen***" auf Seite 143).

Bevor Sie Schichtgeräte hinzufügen, müssen Sie die Schichten für das Basisgerät und die Schichtgeräte aktivieren. Aktivieren Sie die Basisgeräte auf der Seite "Device Settings" (Geräteeinstellungen). Aktivieren Sie die Schichtgeräte auf der Seite "Local Port Settings" (Lokale Porteinstellungen). Sobald die Geräte aktiviert und konfiguriert sind, werden Sie auf der Seite "Port Access" (Portzugriff) (***Seite "Port Access" [Portzugriff]*** (siehe "***Seite "Port Access" (Port-Zugriff)***" auf Seite 48)) angezeigt.

Wenn LX als Basisgerät oder Schichtgerät konfiguriert wurde, wird es wie folgt angezeigt:

- Als Basisgerät konfiguriert: Dies wird im Bereich "Device Information" (Geräteinformationen) im linken Bildschirmbereich der <ProdcutName>-Oberfläche für Basisgeräte angezeigt.
- Als Schichtgerät konfiguriert: Dies wird im Bereich "Device Information" (Geräteinformationen) im linken Bildschirmbereich der <ProdcutName>-Oberfläche für Schichtgeräte angezeigt.
- Das Basisgerät wird als Basis im linken Bildschirmbereich der Schichtgerät-Oberfläche unter "Connect User" (Benutzer verbinden) identifiziert.
- Die Zielverbindungen von der Basis zu einem Schichtport werden als zwei verbundene Ports angezeigt.

Das Basisgerät ermöglicht über eine konsolidierte Portliste auf der Seite "Port Access" (Portzugriff) Remote- und lokalen Zugriff. Schichtgeräte ermöglichen Remotezugriff über ihre eigenen Portlisten. Der lokale Zugriff ist bei Schichtgeräten nicht möglich, wenn "Tiering" (Schichten) aktiviert ist.



Die Portkonfiguration, einschließlich der Änderung des CIM-Namens, muss direkt vom jeweiligen Gerät aus durchgeführt werden. Die Konfiguration von Schichtzielports vom Basisgerät aus ist nicht möglich.

Schichten unterstützen auch die Verwendung von KVM-Switches zum Wechseln zwischen Servern. Siehe ***Konfigurieren von KVM-Switches*** (auf Seite 156).

Aktivieren von Schichten

Verbinden Sie einen Zielserverport auf dem Basisgerät mithilfe eines D2CIM-DVUSB mit dem lokalen Port des LX-Schichtgeräts (Video-/Tastatur-/Mausports).

▶ So aktivieren Sie Schichten:

1. Wählen Sie von der Schichtbasis "Device Settings" > "Device Services" (Geräteeinstellungen > Gerätedienste) aus. Die Seite "Device Service Settings" (Gerätediensteinstellungen) wird angezeigt.
2. Wählen Sie "Enable Tiering as Base" (Schichten als Basis aktivieren) aus.
3. Geben Sie in das Feld "Base Secret" (Geheimer Basisschlüssel) den geheimen Schlüssel ein, der von den Basis- und Schichtgeräten gemeinsam verwendet wird. Dieser geheime Schlüssel ist für die Schichtgeräte zur Authentifizierung des Basisgeräts erforderlich. Sie müssen denselben geheimen Schlüssel für das Schichtgerät eingeben.
4. Klicken Sie auf OK.
5. Aktivieren Sie die Schichtgeräte. Wählen Sie auf dem Schichtgerät "Device Settings" > "Local Port Settings" (Geräteeinstellungen > Lokale Porteinstellungen) aus.
6. Wählen Sie im Bereich "Enable Local Ports" (Lokale Ports aktivieren) die Option "Enable Local Port Device Tiering" (Lokaler Port für Geräteschichten aktivieren) aus.
7. Geben Sie im Feld "Tier Secret" (Geheimer Schlüssel der Schicht) denselben geheimen Schlüssel ein, den Sie für das Basisgerät auf der Seite "Device Settings" (Geräteeinstellungen) eingegeben haben.
8. Klicken Sie auf OK.

Schichten – Zieltypen, unterstützte CIMs und Schichtkonfigurationen

Die Portkonfiguration, einschließlich der Änderung des CIM-Namens, muss direkt vom jeweiligen Gerät aus durchgeführt werden. Die Konfiguration von Schichtzielports vom Basisgerät aus ist nicht möglich.

Nicht unterstützte und eingeschränkte Funktionen auf Schichtzielen

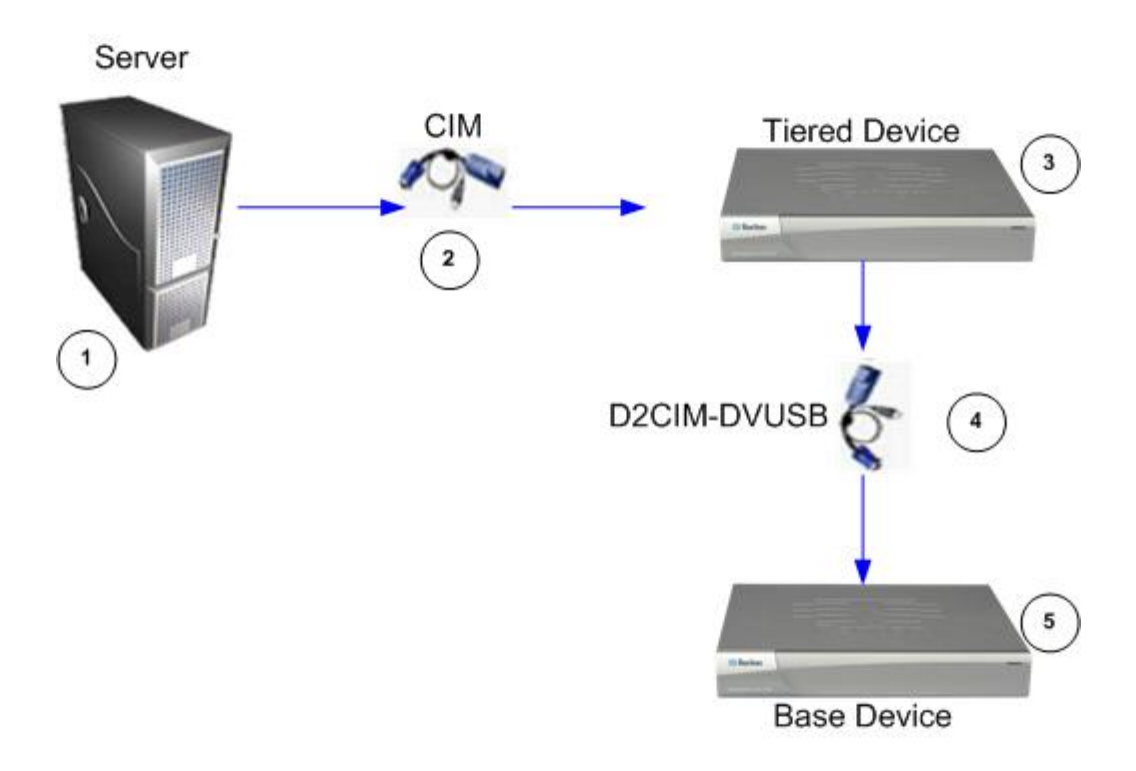
Die folgenden Funktionen werden nicht auf Schichtzielen unterstützt:

- Virtuelle Medien von Schichtgeräten
- MCCAT als Schichtgerät

Verkabelungsbeispiel in Schichtkonfigurationen

Die folgende Abbildung zeigt die Verkabelungskonfigurationen zwischen einem LX-Schichtgerät und einem LX-Basisgerät.

Verbinden Sie einen Zielserverport auf dem Basisgerät mithilfe eines D2CIM-DVUSB mit dem lokalen Port des LX-Schichtgeräts (Video-/Tastatur-/Mausports).



Diagrammschlüssel	
1	Zielserver
2	CIM von Zielserver zum LX-Schichtgerät



Diagrammschlüssel	
3	LX-Schichtgerät
4	D2CIM-DVUSB CIM vom LX-Schichtgerät zum LX-Basisgerät
5	LX-Basisgerät

Aktivieren des direkten Port-Zugriffs über URL

Der direkte Portzugriff ermöglicht es Benutzern, die Verwendung der Seite "Login dialog and Port Access" (Anmeldedialog und Port-Zugriff) zu umgehen. Diese Funktion bietet auch die Möglichkeit, Benutzername und Kennwort direkt einzugeben und das Ziel aufzurufen, wenn Benutzername und Kennwort nicht in der URL enthalten sind.

Wichtige URL-Informationen für den direkten Portzugriff:

Wenn Sie den VKC und direkten Port-Zugriff verwenden:

- https://IP-Adresse/dpa.asp?username=Benutzername&password=Kennwort&port=Port-Nummer

Wenn Sie den AKC und direkten Port-Zugriff verwenden:

- https://IP-Adresse/dpa.asp?username=Benutzername&password=Kennwort&port=Portnummer&client=akc

Dabei gilt:

- Benutzername und Kennwort sind optional. Werden Sie nicht bereitgestellt, wird ein Dialogfeld für die Anmeldung angezeigt. Nach der Authentifizierung wird der Benutzer direkt mit dem Ziel verbunden.
- Für den Port kann eine Port-Nummer oder ein Port-Name angegeben sein. Wenn Sie einen Port-Namen verwenden, muss dieser eindeutig sein, sonst wird ein Fehler gemeldet. Bleibt der Port unberücksichtigt, wird ein Fehler gemeldet.
- "Client=akc" ist optional, außer Sie verwenden den AKC. Wird "Client=akc" nicht verwendet, wird der VKC verwendet.

So aktivieren Sie den direkten Port-Zugriff:

1. Wählen Sie "Device Settings > Device Services" (Geräteeinstellungen > Gerätedienste). Die Seite "Device Service Settings" (Gerätediensteinstellungen) wird geöffnet.



2. Aktivieren Sie die Option "Enable Direct Port Access via URL" (Direkten Port-Zugriff über URL aktivieren), wenn Sie möchten, dass Benutzer über das Dominion-Gerät durch Eingabe der erforderlichen Parameter in die URL direkten Zugriff auf ein Ziel haben.
3. Klicken Sie auf "OK".

Aktivieren der AKC-Download-Serverzertifikat-Validierung

Wenn Sie den AKC verwenden, können Sie wählen, ob Sie die Funktion "Enable AKC Download Server Certificate Validation" (AKC-Download-Serverzertifikat-Validierung aktivieren) verwenden möchten oder nicht.

Option 1: Do Not Enable AKC Download Server Certificate Validation (AKC-Download-Serverzertifikat-Validierung nicht aktivieren [Standardeinstellung])

Wenn Sie die AKC-Download-Serverzertifikat-Validierung nicht aktivieren, alle Benutzer von Dominion-Geräten müssen:

- Stellen Sie sicher, dass die Cookies von der IP-Adresse des Geräts, auf das zugegriffen wird, nicht blockiert werden.
- Die Benutzer von Windows Vista-, Windows 7- und Windows 2008-Servern müssen sicherstellen, dass die IP-Adresse des Geräts, auf das zugegriffen wird, in der Zone "Vertrauenswürdige Sites" hinzugefügt wurde und dass der "Geschützte Modus" nicht aktiv ist, wenn auf das Gerät zugegriffen wird.

Option 2: Enable AKC Download Server Certificate Validation (Übersicht zur AKC-Download-Serverzertifikat-Validierung aktivieren)

Wenn Sie die AKC-Download-Serverzertifikat-Validierung aktivieren:

- Administratoren müssen ein gültiges Zertifikat auf das Gerät hochladen oder ein selbstsigniertes Zertifikat auf dem Gerät generieren. Das Zertifikat muss über eine gültige Hostbezeichnung verfügen.
- Jeder Benutzer muss das CA-Zertifikat (oder eine Kopie des selbstsignierten Zertifikats) zum Speicher für "Vertrauenswürdige Stammzertifizierungsstellen" seines Browsers hinzufügen.

► So installieren Sie das selbstsignierte Zertifikat unter Windows Vista® oder Windows 7®:

1. Fügen Sie die LX-IP-Adresse in der Zone "Vertrauenswürdige Sites" hinzu, und stellen Sie sicher, dass der "Geschützte Modus" nicht aktiv ist.
2. Starten Sie Internet Explorer®, und geben Sie die LX-IP-Adresse als URL ein. Eine Meldung "Zertifikatfehler" wird angezeigt.
3. Wählen Sie "Zertifikate anzeigen" aus.



4. Klicken Sie auf der Registerkarte "Allgemein" auf "Zertifikat installieren". Das Zertifikat wird dann zum Speicher für "Vertrauenswürdige Stammzertifizierungsstellen" hinzugefügt.
5. Nachdem das Zertifikat installiert wurde, kann die LX-IP-Adresse aus der Zone für "Vertrauenswürdige Sites" entfernt werden.

So aktivieren Sie die AKC-Download-Serverzertifikat-Validierung:

1. Wählen Sie "Device Settings > Device Services" (Geräteeinstellungen > Gerätedienste). Die Seite "Device Service Settings" (Gerätediensteinstellungen) wird geöffnet.
2. Aktivieren oder deaktivieren (Standardeinstellung) Sie das Kontrollkästchen "Enable AKC Download Server Certificate Validation" (AKC-Download-Serverzertifikat-Validierung).
3. Klicken Sie auf "OK".

Konfigurieren der Modemeinstellungen

So konfigurieren Sie Modemeinstellungen:

1. Klicken Sie auf "Device Settings" > "Modem Settings" (Geräteeinstellungen > Modemeinstellungen), um die Seite "Modem Settings" (Modemeinstellungen) zu öffnen.
2. Aktivieren Sie das Kontrollkästchen "Enable Modem" (Modem aktivieren). Dadurch werden die Felder "Serial Line Speed" (Geschwindigkeit der seriellen Verbindung) und "Modem Init String" (String für Modeminitialisierung) aktiviert.
3. Die Geschwindigkeit der seriellen Verbindung des Modems ist auf 115200 eingestellt.
4. Geben Sie im Feld "Modem Init String" (String für Modeminitialisierung) die Standardzeichenfolge des Modems ein. Wenn das Feld für die Modemzeichenfolge leer bleibt, wird standardmäßig die folgende Zeichenfolge an das Modem gesendet: ATZ OK AT OK.

   Diese Informationen werden für die Konfiguration der Modemeinstellungen verwendet. Da bei verschiedenen Modems diese Werte auf unterschiedliche Art eingestellt werden, wird in diesem Dokument nicht angegeben, wie diese Werte festgelegt werden. Informationen zum Erstellen der entsprechenden modemspezifischen Zeichenfolge finden Sie in den Unterlagen Ihres Modems.

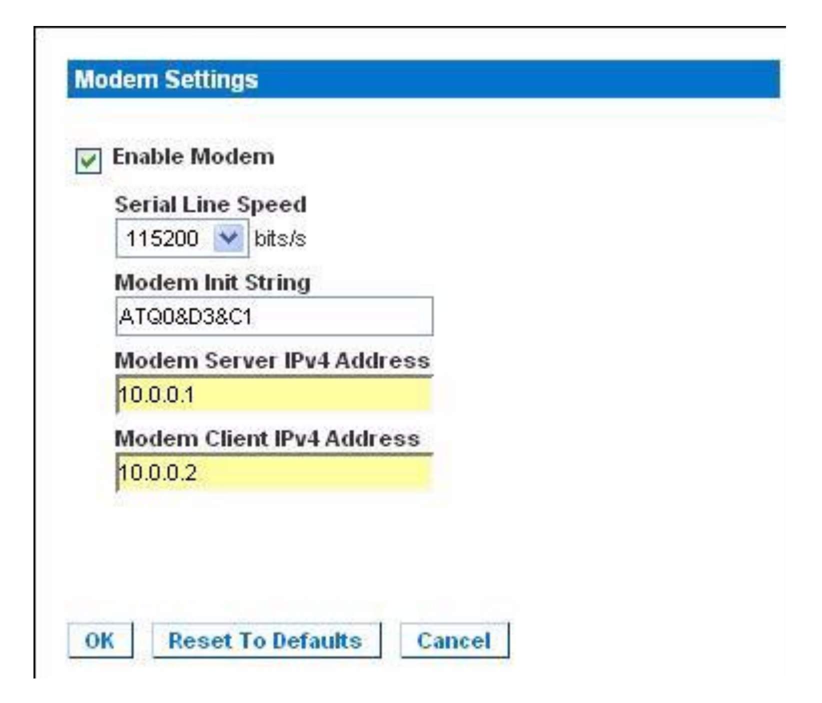
   a. Modemeinstellungen:

- RTS/CTS-Flusssteuerung aktivieren
- Bei Empfang von RTS Daten an den Computer senden
- CTS sollte so konfiguriert sein, dass die Verbindung nur getrennt wird, wenn die Flusssteuerung dies erforderlich macht.
- DTR sollte für Modem-Rücksetzungen mit DTR-Toggle konfiguriert werden.
- DSR sollte immer als "Ein" konfiguriert werden.
- DCD sollte nach Erkennen eines Trägersignals als "Aktiviert" konfiguriert werden (d. h. DCD sollte nur aktiviert werden, wenn eine Modemverbindung mit dem Remotegerät hergestellt wurde).

5. Geben Sie die Modemserver-IPv4-Adresse in das Feld "Modem Server IPv4 Address" (Modemserver-IPv4-Adresse) und die Client-Modemadresse in das Feld "Modem Client IPv4 Address" (Modemclient-IPv4-Adresse) ein.

Hinweis: Die Modemclient- und Server-IP-Adressen müssen sich im gleichen Subnetz befinden und dürfen sich nicht mit dem LAN-Subnetz überschneiden.

6. Klicken Sie auf OK, um Ihre Änderungen zu bestätigen, oder klicken Sie auf "Reset to Defaults" (Auf Standardeinstellungen zurücksetzen), um die Einstellungen auf die Standartwerte zurückzusetzen.





Weitere Informationen zu zertifizierten Modems, die von LX unterstützt werden, finden Sie unter ***Zertifizierte Modems*** (auf Seite 233). Informationen zu Einstellungen für optimale Leistung bei der Verbindung mit LX über ein Modem finden Sie im Abschnitt **"Creating, Modifying and Deleting Profiles in MPC - Generation 2 Devices"** (Erstellen, Ändern und Löschen von Profilen im MPC – Geräte der 2. Generation) des Benutzerhandbuchs **KVM and Serial Access Clients Guide**.

Hinweis: Der direkte Modemzugriff auf die HTML-Oberfläche des LX wird nicht unterstützt. Um über ein Modem auf LX zuzugreifen, müssen Sie eine eigenständige MPC-Anwendung verwenden.

Konfigurieren von Datum-/Uhrzeiteinstellungen

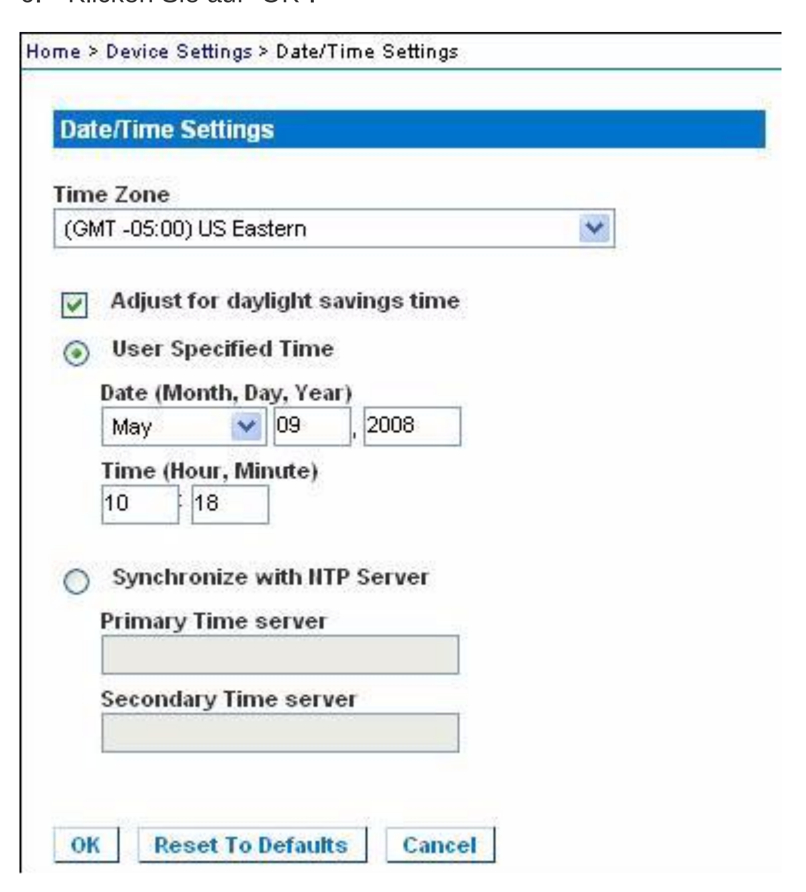
Auf der Seite "Date/Time Settings" (Datum-/Uhrzeiteinstellungen) stellen Sie Datum und Uhrzeit für die LX-Einheit ein. Hierzu haben Sie zwei Möglichkeiten:

- Datum und Uhrzeit manuell einstellen
- Datum und Uhrzeit mit einem NTP (Network Time Protocol)-Server synchronisieren

So stellen Sie das Datum und die Uhrzeit ein:

1. Wählen Sie "Device Settings > Date/Time"(Geräteeinstellungen > Datum/Uhrzeit). Die Seite "Date/Time Settings" (Datum-/Uhrzeiteinstellungen) wird angezeigt.
2. Wählen Sie in der Dropdown-Liste "Time Zone" Ihre Zeitzone aus.
3. Aktivieren Sie das Kontrollkästchen "Adjust for daylight savings time" (an Sommerzeit anpassen), um die Uhrzeit an die Sommerzeit anzupassen.
4. Wählen Sie eine Methode, um Datum und Uhrzeit einzustellen:
   - "User Specified Time" (Benutzerdefinierte Zeit) – Bei dieser Option können Sie Datum und Uhrzeit manuell eingeben. Falls Sie die Option "User Specified Time" (Benutzerdefinierte Zeit) ausgewählt haben, geben Sie Datum und Uhrzeit wie folgt ein: Geben Sie im Feld "Time" die Uhrzeit im Format hh:mm ein. (Verwenden Sie das 24-h-Zeitformat.)
   - "Synchronize with NTP Server" (Mit NTP-Server synchronisieren) – Bei dieser Option können Sie Datum und Uhrzeit mit dem NTP (Network Time Protocol)-Server synchronisieren.
5. Falls Sie die Option "Synchronize with NTP Server" (Mit NTP-Server synchronisieren) ausgewählt haben, gehen Sie folgendermaßen vor:
   a. Geben Sie im Feld "Primary Time Server" (Primärer Zeitserver) die IP-Adresse dieses Servers ein.
   b. Geben Sie im Feld "Secondary Time Server" (Sekundärer Zeitserver) die IP-Adresse dieses Servers ein. ***///Optional***

6. Klicken Sie auf "OK".



Ereignisverwaltung

Das LX-Feature zur Ereignisverwaltung ermöglicht Ihnen die Verteilung von Systemereignissen auf SNMP-Manager, Syslog und das Prüfprotokoll zu aktivieren und zu deaktivieren.



"Event Management - Settings" (Konfigurieren der Ereignisverwaltung – Einstellungen)

SNMP Configuration (SNMP-Konfiguration)

Simple Network Management Protocol (SNMP) ist ein Protokoll für die Netzwerkverwaltung und die Überwachung von Netzwerkgeräten und ihrer Funktionen. LX bietet über die Ereignisverwaltung Unterstützung für SNMP-Agenten.

So konfigurieren Sie SNMP (und aktivieren die SNMP-Protokollierung):

1. Wählen Sie "Device Settings > Event Management - Settings" (Geräteeinstellungen > Ereignisverwaltung - Einstellungen). Die Seite "Event Management – Settings" (Ereignisverwaltung – Einstellungen) wird angezeigt.
2. Wählen Sie "SNMP Logging Enabled" (SNMP-Protokollierung aktiviert) aus. Dadurch werden die übrigen SNMP-Felder aktiviert.
3. Geben Sie in die Felder "Name", "Contact" (Kontakt) und "Location" (Ort) den Namen des SNMP-Agenten (der Name des Geräts), wie er in der LX-Konsolenoberfläche angezeigt wird, einen Kontaktnamen für dieses Gerät und den physischen Ort des Dominion-Geräts ein.
4. Geben Sie im Feld "Agent Community String" (Community-String des Agenten) die Zeichenfolge des Geräts ein. Eine SNMP-Community ist die Gruppe, der Geräte und Verwaltungsstationen angehören, auf denen SNMP ausgeführt wird. Durch sie können Sie leichter definieren, wohin Informationen gesendet werden. Der Community-Name wird zur Identifizierung der Gruppe verwendet. Das SNMP-Gerät oder der SNMP-Agent kann zu mehreren SNMP-Communities gehören.
5. Legen Sie über die Dropdownliste "Type" (Typ) den Lesezugriff (Read-Only) oder den Lese-/Schreibzugriff (Read-Write) für die Community fest.
6. Konfigurieren Sie maximal fünf SNMP-Manager, indem Sie entsprechende Werte in die Felder Destination IP/Hostname (IP-Zieladresse/Hostname), Port # (Port-Nummer) und Community eingeben.
7. Klicken Sie auf den Link "Click here to view the Dominion SNMP MIB" (Klicken Sie hier, um die Dominion-SNMP MIB anzuzeigen), um auf die SNMP Management Information Base zuzugreifen.
8. Klicken Sie auf "OK".

So konfigurieren Sie Syslog und aktivieren die Weiterleitung:

1. Wählen Sie "Enable Syslog Forwarding" (Syslog-Weiterleitung aktivieren) aus, um Geräte-Protokollmeldungen an einen Remote-Syslog-Server zu senden.
2. Geben Sie die IP-Adresse/den Hostnamen Ihres Syslog-Servers im Feld "IP Address" (IP-Adresse) ein.
3. Klicken Sie auf "OK".



▶ So stellen Sie die werksseitigen Standardeinstellungen wieder her:

- Klicken Sie auf "Reset to Defaults" (Standardeinstellungen wiederherstellen).

Hinweis: IPv6-Adressen dürfen maximal 80 Zeichen umfassen.

Home > Device Settings > Event Management - Settings

SNMP Configuration

☐ SNMP Logging Enabled

Name

LX

Contact

Location

Agent Community String

Type

Read-Only

Destination IP/Hostname	Port #	Community
	162	public
	162	public
	162	public
	162	public
	162	public

Click here to view the Dominion LX SNMP MIB

SysLog Configuration

☐ Enable Syslog Forwarding

IP Address/Host Name

OK | Reset To Defaults | Cancel

Konfiguration von Ports

Die Seite "Port Configuration" (Port-Konfiguration) enthält eine Liste der LX-Ports. Die mit KVM-Zielservern verbundenen Ports werden in blau angezeigt. Ports, an die kein CIM angeschlossen oder für die kein CIM-Name angegeben ist, wird der Standardportname "Dominion-LX_Port#" zugewiesen, wobei "Port#" für die Nummer des physischen LX-Ports steht.

Wenn der Status eines Ports ausgeschaltet ist, wird dafür "Not Available" (Nicht verfügbar) angezeigt. Ein Port kann ausgeschaltet sein, wenn das CIM des Ports entfernt oder ausgeschaltet wurde.

Nach dem Umbenennen des Ports können Sie den Standardportnamen jederzeit mit der Schaltfläche "Reset to Default" (Auf Standard zurücksetzen) wiederherstellen.

So greifen Sie auf eine Portkonfiguration zu:

1. Wählen Sie "Device Settings > Port Configuration" (Geräteeinstellungen > Port-Konfiguration). Die Seite "Port Configuration" (Portkonfiguration) wird angezeigt.

   Der Inhalt der Seite wird zunächst in der Reihenfolge der Port-Nummern angezeigt. Sie können für eine andere Sortierung jedoch auf eine der Spaltenüberschriften klicken.

   - Port Number (Portnummer) – Die für das LX-Gerät verfügbaren Ports werden beginnend mit 1 durchnummeriert.
   - "Port Name" (Portname) – Der dem Port zugewiesene Name. Sie können Ports auch umbenennen, die aktuell nicht über ein CIM mit LX verbunden sind und daher den Status "Not Available" (Nicht verfügbar) haben. Führen Sie zum Umbenennen eines Ports mit dem Status "Not Available" (Nicht verfügbar) einen der folgenden Schritte aus:
     - Benennen Sie den Port um. Beim Anhängen eines CIM wird der CIM-Name verwendet.
     - Benennen Sie den Port um, und wählen Sie "Persist name on Next CIM Insertion" (Name bei nächster CIM-Installation beibehalten). Beim Anhängen eines CIM wird der zugewiesene Name in das CIM kopiert.
     - Setzen Sie den Port durch Auswählen der Option "Reset to Defaults" (Auf werksseitige Standardeinstellungen zurücksetzen) auf die werksseitigen Standardeinstellungen zurück. Beim Anhängen eines CIM wird der CIM-Name verwendet.

   Hinweis: Verwenden Sie für den Port (CIM)-Namen keine Auslassungszeichen (Apostroph).



- Port-Typ:
  - DCIM – Dominion-CIM
  - "Not Available" (Nicht verfügbar) – Kein CIM angeschlossen
  - MCUTP – Master Console MCUTP, CIM in Kabel
  - PCIM – Paragon-CIM
  - Dual -VM – Virtuelle Medien-CIM (D2CIM-VUSB und D2CIM-DVUSB)
  - KVM-Switch – Generische KVM-Switch-Verbindung

2. Klicken Sie auf den Portnamen des Ports, den Sie bearbeiten möchten. Die Seite "Port" für KVM wird angezeigt.

Konfigurieren von Standardzielservern

So benennen Sie die Zielserver:

1. Schließen Sie alle Zielserver an, falls dies noch nicht geschehen ist. Weitere Einzelheiten finden Sie unter ***Schritt 3: Anschließen der Geräte*** (siehe "***Schritt 3: Anschließen der Geräte***" auf Seite 30) für eine Beschreibung zum Anschließen der Geräte.
2. Wählen Sie "Device Settings" > "Port Configuration" (Geräteeinstellungen > Portkonfiguration) aus. Die Seite "Port Configuration" (Portkonfiguration) wird angezeigt.
3. Klicken Sie auf den Portnamen des Zielservers, den Sie umbenennen möchten. Die Seite "Port" wird angezeigt.
4. Wählen Sie "Standard KVM Port" als Subtyp für den Port aus.
5. Weisen Sie dem mit diesem Port verbundenen Server einen Namen zu. Der Name darf maximal 32 alphanumerische Zeichen oder Sonderzeichen umfassen.
6. Wählen Sie im Bereich "Target Settings" (Zieleinstellungen) die Option "720x400 Compensation" (720x400-Kompensierung) aus, wenn das Ziel diese Auflösung verwendet und Anzeigeprobleme auftreten.
7. Wählen Sie "Use international keyboard for scan code set 3" (Internationale Tastatur für Scancode Satz 3 verwenden) aus, wenn Sie mit einem DCIM-PS2 die Verbindung zum Ziel herstellen und den Scancode Satz 3 mit einer internationalen Tastatur verwenden müssen.
8. Klicken Sie auf "OK".



Konfigurieren von KVM-Switches

LX ermöglicht das Einfügen von Schichten in generischen, analogen KVM-Switches, die die Funktion zum Wechseln über Zugriffstasten unterstützen. Es stehen viele verschiedene KVM-Tastenfolgen zum Wechseln zur Verfügung. Wählen Sie eine Option aus, die mit der Tastenfolge zum Wechseln übereinstimmt, die vom analogen KVM-Switch unterstützt wird, zu dem eine Verbindung über diesen Port besteht. Dadurch werden Ziele auf dem analogen Schicht-KVM-Switch über eine konsolidierte Portliste auf der Seite "Port Access" (Portzugriff) zugänglich.

Wichtig: Damit die Benutzergruppen den von Ihnen erstellten KVM-Switch sehen können, müssen Sie zuerst den Switch und dann die Gruppe erstellen. Wenn eine vorhandene Benutzergruppe den von Ihnen erstellten KVM-Switch sehen muss, müssen Sie die Benutzergruppe neu erstellen.

So konfigurieren Sie KVM-Switches:

1. Wählen Sie "Device Settings > Port Configuration" (Geräteeinstellungen > Port-Konfiguration). Die Seite "Port Configuration" (Port-Konfiguration) wird angezeigt.
2. Klicken Sie auf den Portnamen des Zielservers, den Sie umbenennen möchten. Die Seite"Port" (Port) wird angezeigt.
3. Wählen Sie den KVM-Switch aus.
4. Wählen Sie das KVM-Switch-Modell aus.

   Hinweis: Es wird nur ein Switch in der Dropdown-Liste angezeigt.

5. Wählen Sie "KVM Switch Hot Key Sequence" (KVM-Switch-Tastenfolge) aus.
6. Geben Sie die maximale Anzahl der Zielports (2-32) ein.
7. Geben Sie im Feld "KVM Switch Name" den gewünschten Namen für diese Portkonfiguration ein.
8. Aktivieren Sie die Ziele für die KVM-Switch-Tastenfolge. Geben Sie die KVM-Switch-Ports mit angeschlossenen Zielen an, indem Sie für jeden Port die Option "Active" (Aktiv) auswählen.
9. Im Abschnitt "KVM Managed Links" (Verwaltete KVM-Verknüpfungen) der Seite können Sie die Verbindung zu einer Webbrowseroberfläche konfigurieren, wenn verfügbar.



a. "Active" (Aktiv) – Aktivieren Sie das Kontrollkästchen "Active" (Aktiv), um die Verknüpfung nach der Konfiguration zu aktivieren. Aktiveren Sie das Kontrollkästchen nicht, wenn die Verknüpfung inaktiv bleiben soll. In die Verknüpfungsfelder können Informationen auch dann eingegeben und gespeichert werden, wenn "Active" (Aktiv) nicht ausgewählt wurde. Wenn "Active" (Aktiv) ausgewählt wurde, muss im URL-Feld eine Eingabe vorgenommen werden. Benutzername, Kennwort sowie die Felder "Username" (Benutzername) und "Password" (Kennwort) sind optional (abhängig davon, ob eine Einzelanmeldung gewünscht wird oder nicht).

b. "URL Name" (URL-Name) – Geben Sie die URL zur Benutzeroberfläche ein.

c. "Username" (Benutzername) – Geben Sie den Benutzernamen ein, der für den Zugriff auf die Benutzeroberfläche verwendet wird.

d. "Password" (Kennwort) – Geben Sie das Kennwort ein, das für den Zugriff auf die Benutzeroberfläche verwendet wird.

e. Feld "Username" (Benutzername) - Geben Sie den Parameter des Benutzernamens ein, der in der URL verwendet wird. Beispielsweise *username*=admin, wobei *username* das Feld "username" (Benutzername) ist.

f. Feld "Password" (Kennwort) - Geben Sie den Parameter des Kennworts ein, der in der URL verwendet wird. Beispielsweise *password*=raritan, wobei *password* das Feld "password " (Kennwort) ist.

10. Klicken Sie auf "OK".

So ändern Sie den aktiven Status eines KVM-Switch-Ports oder einer URL:

1. Wählen Sie "Device Settings > Port Configuration" (Geräteeinstellungen > Port-Konfiguration). Die Seite "Port Configuration" (Port-Konfiguration) wird angezeigt.
2. Klicken Sie auf den Portnamen des Zielservers, den Sie umbenennen möchten. Die Seite"Port" (Port) wird angezeigt.
3. Deaktivieren Sie das Kontrollkästchen "Active" (Aktiv) neben dem KVM-Switch-Zielport oder neben der URL, um den aktiven Status zu ändern.
4. Klicken Sie auf "OK".

Lokale Porteinstellungen für LX konfigurieren

Auf der Seite "Local Port Settings" (Lokale Porteinstellungen) können Sie viele Einstellungen für die lokale LX-Konsole anpassen. Dazu zählen die Tastatur, die Zugriffstasten, die Verzögerung beim Videowechsel, der Stromsparmodus, die Auflösungseinstellungen für die lokale Benutzeroberfläche sowie die lokale Benutzerauthentifizierung.

So konfigurieren Sie die lokalen Porteinstellungen:

Hinweis: Einige Einstellungsänderungen, die auf der Seite "Local Port Settings" (Lokale Porteinstellungen) vorgenommen werden, führen zum Neustart des verwendeten Browsers. Führt eine Einstellungsänderung zum Neustart des Browser, so ist dies in den hier beschriebenen Schritten vermerkt.

1. Wählen Sie "Device Settings" > "Local Port Settings" (Geräteeinstellungen > Lokale Porteinstellungen) aus. Die Seite "Local Port Settings" (Lokale Porteinstellungen) wird angezeigt.
2. Aktivieren Sie das Kontrollkästchen neben "Enable Standard Local Port" (Lokalen Standardport aktivieren). Deaktivieren Sie das Kontrollkästchen, um den Port zu deaktivieren. Der lokale Standardport ist standardmäßig aktiviert, kann jedoch bei Bedarf aktiviert werden. Der Browser wird neu gestartet, nachdem diese Änderung durchgeführt wurde. Wenn Sie die Schichtfunktion verwenden, ist diese Funktion deaktiviert, da beide Funktionen nicht gleichzeitig verwendet werden können.
3. Wenn Sie die Schichtfunktion verwenden, wählen Sie das Kontrollkästchen "Enable Local Port Device Tiering" (Geräteschicht für lokalen Port aktivieren) aus und geben den geheimen Schlüssel für die Schicht in das Feld "Tier Secret" (Geheimer Schlüssel der Schicht) ein. Um die Schichten zu konfigurieren, müssen Sie auch das Basisgerät auf der Seite "Device Services" (Gerätedienste) konfigurieren. Weitere Informationen zu Schichten finden Sie unter ***Konfigurieren und Aktivieren von Schichten*** (auf Seite 142).
4. Konfigurieren Sie ggf. die Einstellungen "Local Port Scan Mode" (Scanmodus für den lokalen Port). Diese Einstellungen gelten für das Feature "Scan Settings" (Scaneinstellungen), auf das Sie über die Seite "Port" zugreifen. Siehe ***Scannen von Ports*** (auf Seite 51).
   - Geben Sie im Feld "Display Interval (10-255 sec):" (Anzeigeintervall (10-255 Sek.)) die Anzahl Sekunden ein, die das Ziel im Fokus in der Mitte des Fensters "Port Scan" (Port-Scan) angezeigt werden soll.
   - Geben Sie im Feld "Interval Between Ports (10 - 255 sec):" (Intervall zwischen Ports (10 – 255 Sek.)) das Intervall ein, in dem das Gerät zwischen Ports pausieren soll.



5. Wählen Sie aus den Optionen in der Dropdown-Liste den geeigneten Tastaturtyp aus. Der Browser wird neu gestartet, nachdem diese Änderung durchgeführt wurde.
   - US
   - US/International (USA/International)
   - United Kingdom (Großbritannien)
   - French (France) (Französisch)
   - German (Germany) (Deutsch)
   - JIS (Japanese Industry Standard) (Japanisch [Japanischer Branchenstandard])
   - Simplified Chinese (Vereinfachtes Chinesisch)
   - Traditional Chinese (Traditionelles Chinesisch)
   - Dubeolsik Hangul (Korean) (Koreanisch)
   - German (Deutsch, Schweiz)
   - Portugiesisch (Portugal)
   - Norwegian (Norway) (Norwegisch)
   - Swedish (Sweden) (Schwedisch)
   - Danish (Denmark) (Dänisch)
   - Belgian (Belgium) (Belgisch)

Hinweis: Sie können die Tastatur für Chinesisch, Japanisch und Koreanisch nur für die Anzeige verwenden. Für Funktionen der lokalen LX-Konsole werden Eingaben in diesen Sprachen derzeit nicht unterstützt.

Hinweis: Bei Verwendung einer türkischen Tastatur müssen Sie die Verbindung mit einem Zielserver über den Active KVM Client (AKC) herstellen. Von anderen Raritan-Clients wird es nicht unterstützt.

6. Wählen Sie die Zugriffstaste für den lokalen Port. Über die Zugriffstaste für den lokalen Port können Sie zur Benutzeroberfläche der lokalen LX-Konsole zurückkehren, wenn gerade eine Zielserveroberfläche angezeigt wird. Die Standardoption lautet "Double Click Scroll Lock" (Rollen-Taste zweimal drücken). Sie können jedoch eine andere Tastenkombination aus der Dropdownliste auswählen.

Zugriffstaste	**Zu drückende Tastenkombination**
Rollen-Taste zweimal drücken	Drücken Sie die Rollen-Taste zweimal kurz hintereinander.
Num-Feststelltaste zweimal drücken	Drücken Sie die Num-Feststelltaste zweimal kurz hintereinander.



Zugriffstaste	Zu drückende Tastenkombination
Feststelltaste zweimal drücken	Drücken Sie die Feststelltaste zweimal kurz hintereinander.
Linke Alt-Taste zweimal drücken	Drücken Sie die linke Alt-Taste zweimal kurz hintereinander.
Linke Umschalttaste zweimal drücken	Drücken Sie die linke Umschalttaste zweimal kurz hintereinander.
Linke Strg-Taste zweimal drücken	Drücken Sie die linke Strg-Taste zweimal kurz hintereinander.

7. Wählen Sie die Verbindungstaste für den lokalen Port aus. Verwenden Sie eine Verbindungstastenfolge, um eine Verbindung mit einem Zielgerät herzustellen und zu einem anderen Zielgerät zu wechseln. Sie können anschließend die Zugriffstaste verwenden, um die Verbindung zum Zielgerät zu trennen und zur GUI des lokalen Ports zurückzukehren. Wenn die Verbindungstaste für den lokalen Port erstellt wurde, erscheint diese im Navigationsfenster der GUI, sodass Sie sie als Referenz verwenden können. Beispiele für Verbindungstastenfolgen finden Sie unter Beispiele für Verbindungstasten.
8. Legen Sie ggf. im Feld "Video Switching Delay" (Verzögerung beim Videowechsel) einen Wert zwischen 0 und 5 Sekunden fest. Üblicherweise wird der Wert 0 verwendet, wenn nicht mehr Zeit benötigt wird (manche Monitore benötigen mehr Zeit, um das Videobild zu wechseln).
9. Führen Sie die folgenden Schritte aus, falls Sie das Stromsparfeature verwenden möchten:
   a. Aktivieren Sie das Kontrollkästchen "Power Save Mode" (Stromsparmodus).
   b. Legen Sie die Zeitspanne (in Minuten) fest, nach der in den Stromsparmodus geschaltet wird.
10. Wählen Sie in der Dropdown-Liste die Auflösung für die lokale LX-Konsole aus: Der Browser wird neu gestartet, nachdem diese Änderung durchgeführt wurde.
    - 800x600
    - 1024x768
    - 1280x1024
11. Wählen Sie in der Dropdown-Liste die Aktualisierungsfrequenz aus. Der Browser wird neu gestartet, nachdem diese Änderung durchgeführt wurde.
    - 60 Hz
    - 75 Hz



12. Wählen Sie die Methode zur lokalen Benutzerauthentifizierung aus:
    - Local/LDAP/RADIUS (Lokal/LDAP/RADIUS): Dies ist die empfohlene Option. Weitere Informationen zur Authentifizierung finden Sie unter ***Remoteauthentifizierung*** (auf Seite 38).
    - Keine. Der lokale Konsolenzugriff wird nicht authentifiziert. Diese Option ist nur für sichere Umgebungen empfehlenswert.
13. Klicken Sie auf "OK".

Ändern der Standardeinstellung für die GUI-Sprache

Die grafische Benutzeroberfläche (GUI) von LX unterstützt die folgenden lokalisierten Sprachen:

- Japanese (Japanisch)
- Simplified Chinese (Vereinfachtes Chinesisch)
- Traditional Chinese (Traditionelles Chinesisch)

So ändern Sie die GUI-Sprache:

1. Wählen Sie "Device Settings" (Geräteeinstellungen) > "Language" (Sprache). Die Seite "Language Settings" (Spracheinstellungen) wird angezeigt.
2. Wählen Sie in der Dropdownliste "Language" (Sprache) die Sprache für die GUI aus.
3. Klicken Sie auf "Apply" (Übernehmen). Klicken Sie auf "Reset to Defaults" (Standardeinstellungen wiederherstellen), um die Sprache wieder auf "English" (Englisch) zurückzusetzen.

Hinweis: Sobald Sie eine neue Sprache übernehmen, wird die Online-Hilfe ebenfalls Ihrer Sprachauswahl entsprechend lokalisiert.

Kapitel 7 Sicherheitsverwaltung

In diesem Kapitel

"Security Settings" (Sicherheitseinstellungen)

Auf der Seite "Security Settings" (Sicherheitseinstellungen) können Sie Anmeldebeschränkungen angeben, Benutzer blockieren, Kennwortregeln festlegen und Daten verschlüsseln und freigeben.

Für den Austausch öffentlicher und privater Schlüssel werden SSL-Zertifikate von Raritan verwendet, die zusätzliche Sicherheit bieten. Raritan-Webserverzertifikate sind selbstsigniert. Java-Applet-Zertifikate sind durch ein VeriSign-Zertifikat signiert. Die Verschlüsselung stellt sicher, dass Ihre Informationen nicht in falsche Hände geraten, und anhand dieser Zertifikate sehen Sie, dass es sich um Raritan, Inc. handelt.

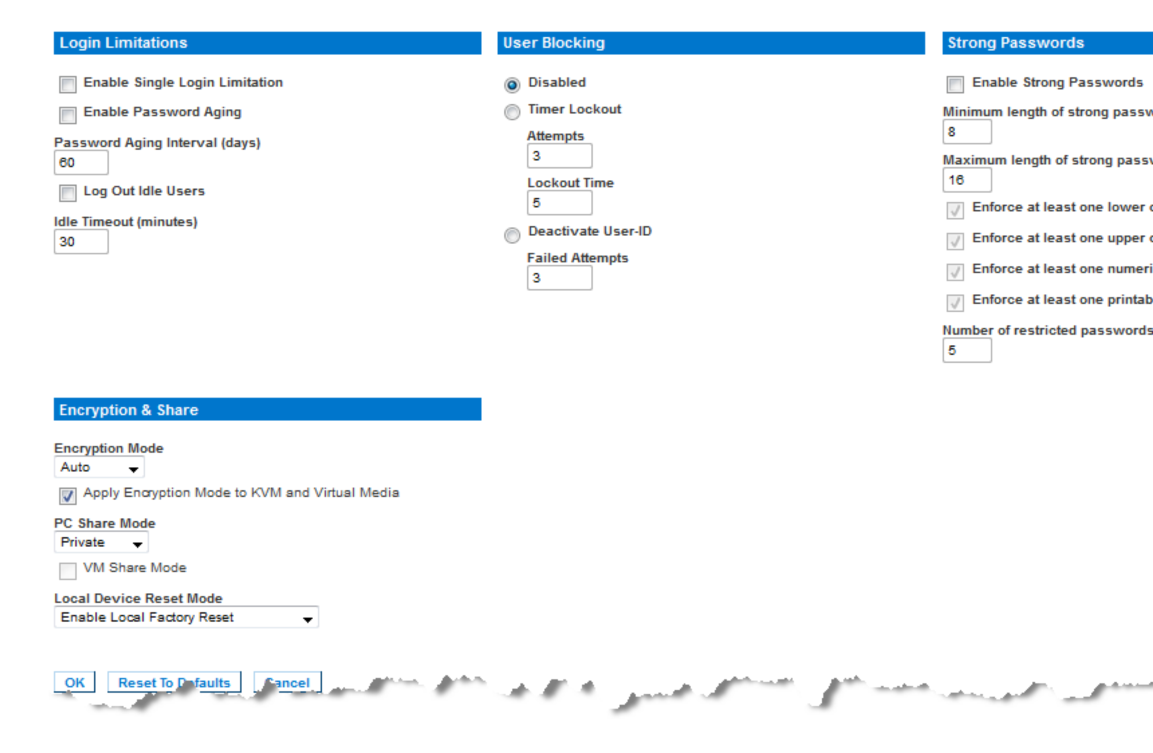
So konfigurieren Sie die Sicherheitseinstellungen:

1. Wählen Sie "Security" > "Security Settings" (Sicherheit > Sicherheitseinstellungen) aus. Die Seite "Security Settings" (Sicherheitseinstellungen) wird angezeigt.
2. Aktualisieren Sie ggf. die Einstellungen unter ***Login Limitations (Anmeldebeschränkungen)*** (siehe "***Anmeldebeschränkungen***" auf Seite 163).
3. Aktualisieren Sie ggf. die Einstellungen unter ***Strong Passwords (Sichere Kennwörter)*** (auf Seite 165).
4. Aktualisieren Sie ggf. die Einstellungen für ***User Blocking (Benutzersperrung)*** (auf Seite 166).
5. Aktualisieren Sie ggf. die Einstellungen unter ***Encryption & Share (Verschlüsselung und Freigabe)*** (auf Seite 168).
6. Klicken Sie auf OK.



So stellen Sie die Standardwerte wieder her:

- Klicken Sie auf "Reset to Defaults" (Standardeinstellungen wiederherstellen).



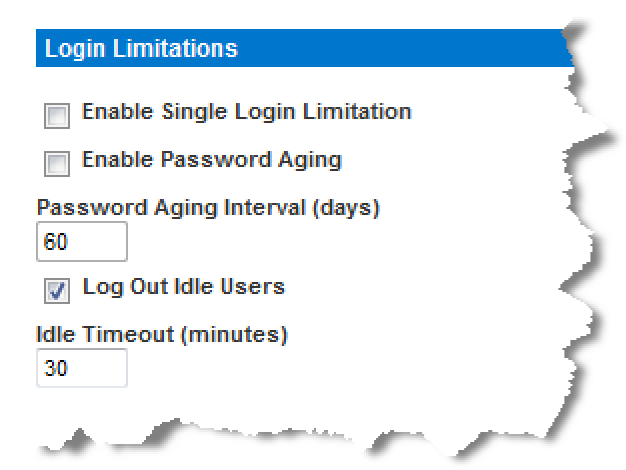
Anmeldebeschränkungen

Mithilfe von Anmeldebeschränkungen können Sie Beschränkungen für Einzelanmeldungen, die Geltungsdauer von Kennwörtern und das Abmelden inaktiver Benutzer festlegen.

Beschränkung	Beschreibung
"Enable single login limitation" (Beschränkung für Einzelanmeldung aktivieren)	Wenn Sie dieses Kontrollkästchen aktivieren, ist pro Benutzername immer nur eine Anmeldung zulässig. Ist es dagegen deaktiviert, kann eine Benutzername-/Kennwortkombination von mehreren Client-Workstations gleichzeitig verwendet werden, um eine Verbindung mit dem Gerät herzustellen.
"Enable Password Aging" (Erneuerung des Kennworts aktivieren)	Wenn Sie dieses Kontrollkästchen aktivieren, müssen alle Benutzer ihr Kennwort abhängig von der Anzahl der Tage, die Sie im Feld "Password Aging Interval" (Intervall für Kennworterneuerung) eingegeben haben, regelmäßig ändern. Dieses Feld ist aktiv und erforderlich, wenn Sie



Beschränkung	Beschreibung
	das Kontrollkästchen "Enable Password Aging" (Erneuerung des Kennworts aktivieren) aktiviert haben. Geben Sie den Zeitraum in Tagen an, nach dessen Ablauf ein Kennwort geändert werden muss. Der Standardwert ist 60 Tage.
"Log out idle users, After (1-365 minutes)" (Inaktive Benutzer abmelden, Nach (1-365 Minuten))	Aktivieren Sie das Kontrollkästchen "Log off idle users" (Inaktive Benutzer abmelden), um die Verbindung von Benutzern automatisch zu trennen, wenn der im Feld "After (1-365 minutes)" [Nach (1-365 Minuten)] angegebene Zeitraum abgelaufen ist. Wenn keine Tastatur- oder Mausaktivitäten stattfinden, werden alle Sitzungen und Ressourcen abgemeldet. Für virtuelle Mediensitzungen gibt es hingegen kein Zeitlimit. Das Feld "After" (Nach) dient zum Festlegen der Zeitspanne (in Minuten), nach der ein inaktiver Benutzer abgemeldet wird. Dieses Feld ist aktiv, wenn Sie das Kontrollkästchen "Log Out Idle Users" (Inaktive Benutzer abmelden) aktiviert haben. Als Feldwert können bis zu 365 Minuten eingegeben werden.





Strong Passwords (Sichere Kennwörter)

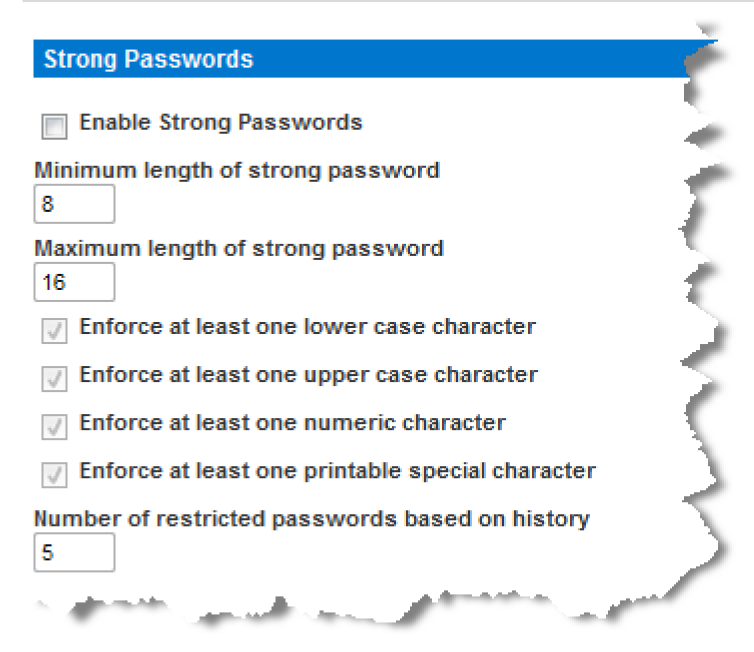
Sichere Kennwörter sorgen für eine sicherere lokale Authentifizierung des Systems. Im Bereich "Strong Passwords" (Sichere Kennwörter) können Sie das Format gültiger lokaler LX-Kennwörter wie Mindest- und Höchstlänge, erforderliche Zeichen und Aufbewahrung des Kennwortverlaufs festlegen.

Damit ein Kennwort sicher ist, muss es eine Mindestlänge von acht Zeichen haben sowie mindestens ein alphabetisches Zeichen und ein nicht-alphabetisches Zeichen (Satzzeichen oder Ziffer) umfassen. Darüber hinaus dürfen die ersten vier Zeichen des Kennworts und des Benutzernamens nicht identisch sein.

Wenn Sie diese Option aktivieren, gelten die Regeln für sichere Kennwörter. Benutzer, deren Kennwörter nicht den Kriterien für sichere Kennwörter entsprechen, werden bei der nächsten Anmeldung automatisch aufgefordert, ihr Kennwort zu ändern. Ist das Kontrollkästchen deaktiviert, gilt nur die Standardformatvalidierung. Bei aktiviertem Kontrollkästchen sind die folgenden Felder aktiv und erforderlich:

Feld	Beschreibung
Minimum length of strong password (Mindestlänge des sicheren Kennworts)	Kennwörter müssen mindestens 8 Zeichen umfassen. Es dürfen aber bis zu 63 Zeichen sein.
Maximum length of strong password (Höchstlänge des sicheren Kennworts)	Kennwörter müssen mindestens 8 und dürfen maximal 16 Zeichen umfassen.
Enforce at least one lower case character (Mindestens einen Kleinbuchstaben erzwingen)	Wenn dieses Kontrollkästchen aktiviert ist, muss das Kennwort mindestens einen Kleinbuchstaben enthalten.
Enforce at least one upper case character (Mindestens einen Großbuchstaben erzwingen)	Wenn dieses Kontrollkästchen aktiviert ist, muss das Kennwort mindestens einen Großbuchstaben enthalten.
Enforce at least one numeric character (Mindestens eine Ziffer erzwingen)	Wenn dieses Kontrollkästchen aktiviert ist, muss das Kennwort mindestens eine Ziffer enthalten.
Enforce at least one printable special character (Mindestens ein druckbares Sonderzeichen erzwingen)	Wenn dieses Kontrollkästchen aktiviert ist, muss das Kennwort mindestens ein (druckbares) Sonderzeichen enthalten.
Number of restricted passwords based on history	Dieses Feld bezieht sich auf die Verlaufstiefe, d. h. die Anzahl vorheriger

Feld	Beschreibung
(Anzahl unzulässiger Kennwörter basierend auf Verlauf)	Kennwörter, die nicht wiederholt werden dürfen. Ein Bereich zwischen 1 und 12 ist möglich, der Standardwert liegt bei 5.



User Blocking (Benutzersperrung)

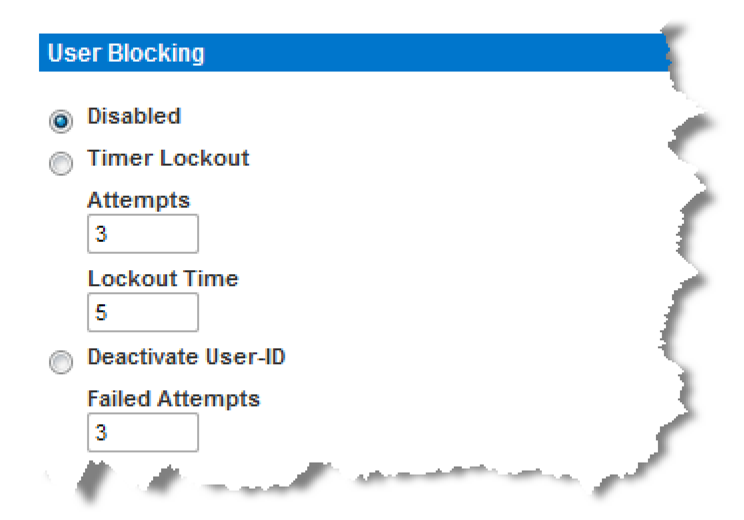
Mithilfe der Optionen unter "User Blocking" (Benutzersperrung) geben Sie die Kriterien an, anhand derer Benutzer nach der festgelegten Zahl von Anmeldefehlversuchen am Zugriff auf das System gehindert werden.

Die drei Optionen schließen sich gegenseitig aus.

Option	Beschreibung
"Disabled" (Deaktiviert)	Dies ist die Standardoption. Benutzer werden unabhängig von der Anzahl fehlgeschlagener Anmeldeversuche nicht blockiert.



Option	Beschreibung
"Timer Lockout" (Zeitliche Sperre)	Benutzern wird der Zugriff auf das System für den festgelegten Zeitraum verweigert, nachdem sie eine bestimmte Anzahl von Anmeldefehlversuchen überschritten haben. Bei dieser Option stehen die folgenden Felder zur Verfügung: ▪ "Attempts" (Versuche) – Geben Sie die Anzahl fehlgeschlagener Anmeldeversuche ein, nach der ein Benutzer gesperrt wird. Ein Bereich zwischen 1 und 10 ist möglich, der Standardwert liegt bei 3 Versuchen. ▪ "Lockout Time" (Dauer der Sperre) – Geben Sie die Zeitspanne ein, für die der Benutzer gesperrt wird. Ein Bereich zwischen 1 und 1.440 Minuten ist möglich, der Standardwert liegt bei 5 Minuten. *Hinweis: Administratoren sind von einer zeitlichen Sperre ausgenommen.*
"Deactivate User-ID" (Benutzer-ID deaktivieren)	Diese Option legt fest, dass dem Benutzer nach der Anzahl der im Feld "Failed Attempts" (Fehlversuche) angegebenen Anmeldefehlversuche der Zugriff auf das System verweigert wird. ▪ "Failed Attempts" (Fehlversuche) – Geben Sie die Anzahl der Anmeldefehlversuche ein, nach der die Benutzer-ID eines Benutzers deaktiviert wird. Dieses Feld steht zur Verfügung, wenn Sie die Option "Deactivate User-ID" (Benutzer-ID deaktivieren) wählen. Der gültige Bereich liegt zwischen 1 und 10. Wenn eine Benutzer-ID nach der angegebenen Anzahl der Anmeldefehlversuche deaktiviert wird, muss der Administrator das Benutzerkennwort ändern und das Benutzerkonto wieder aktivieren, indem er auf der Seite "User" (Benutzer) das Kontrollkästchen "Active" (Aktiv) aktiviert.



Encryption & Share (Verschlüsselung und Freigabe)

Mithilfe der Einstellungen unter "Encryption & Share" (Verschlüsselung und Freigabe) können Sie die Art der Verschlüsselung, PC- und VM-Freigabemodi sowie die Art der Zurücksetzung festlegen, wenn die Taste "Reset" (Zurücksetzen) an der LX-Einheit gedrückt wird.

WARNUNG: Wenn Sie einen Verschlüsselungsmodus auswählen, der von Ihrem Browser nicht unterstützt wird, können Sie von Ihrem Browser aus nicht auf LX zugreifen.

So konfigurieren Sie die Verschlüsselung und Freigabe:

1. Wählen Sie eine Option aus der Dropdownliste "Encryption Mode" (Verschlüsselungsmodus) aus. Wenn Sie einen Verschlüsselungsmodus ausgewählt haben, wird eine Warnung angezeigt, dass Sie keine Verbindung zu LX mehr herstellen können, falls Ihr Browser den gewählten Modus nicht unterstützt. Die Warnung lautet "When the Encryption Mode is specified please ensure that your browser supports this encryption mode; otherwise you will not be able to connect to the LX" (Wenn Sie den Verschlüsselungsmodus festlegen, stellen Sie sicher, dass Ihr Browser diesen unterstützt, ansonsten können Sie keine Verbindung zu LX herstellen).

Verschlüsselungsmodus	Beschreibung
Automatisch	Dies ist die empfohlene Option. LX verwendet automatisch das höchstmögliche Verschlüsselungsniveau.



Verschlüsselung smodus	Beschreibung
RC4	Sichert Benutzernamen, Kennwörter und KVM-Daten einschließlich Videoübertragungen mithilfe der Verschlüsselungsmethode RSA RC4. Dies ist ein 128-Bit-SSL-Protokoll (Secure Sockets Layer), das während der Anfangsverbindungsauthentifizierung einen privaten Kommunikations-Channel zwischen dem LX-Gerät und dem Remote-PC bereitstellt.
AES-128	Der Advanced Encryption Standard (AES) ist eine Spezifikation des National Institute of Standards and Technology (USA) für die Verschlüsselung elektronischer Daten. 128 ist die Schlüssellänge. Achten Sie bei Auswahl dieser Option (AES-128) darauf, dass sie von Ihrem Browser unterstützt wird, da Sie sonst keine Verbindung herstellen können. Weitere Informationen finden Sie unter ***Prüfen Ihres Browsers auf AES-Verschlüsselung*** (auf Seite 171).
AES-256	Der Advanced Encryption Standard (AES) ist eine Spezifikation des National Institute of Standards and Technology (USA) für die Verschlüsselung elektronischer Daten. 256 ist die Schlüssellänge. Achten Sie bei Auswahl dieser Option (AES-256) darauf, dass sie von Ihrem Browser unterstützt wird, da Sie sonst keine Verbindung herstellen können. Weitere Informationen finden Sie unter ***Prüfen Ihres Browsers auf AES-Verschlüsselung*** (auf Seite 171).

Hinweis: Der MPC verwendet immer das höchste Verschlüsselungsniveau und entspricht der Einstellung unter "Encryption Mode" (Verschlüsselungsmodus), wenn diese nicht auf "Auto" eingestellt ist.

Hinweis: Wenn Sie Windows XP® mit Service Pack 2 verwenden, kann der Internet Explorer® 7 keine Remoteverbindung zu LX herstellen, wenn die AES-128-Verschlüsselung verwendet wird.

2. Apply Encryption Mode to KVM and Virtual Media (Verschlüsselungsmodus auf KVM und virtuelle Medien anwenden): Wenn Sie dieses Kontrollkästchen aktivieren, wird der gewählte Verschlüsselungsmodus auf KVM und virtuelle Medien angewendet. Nach der Authentifizierung werden die KVM- und virtuellen Mediendaten ebenfalls mit der 128-Bit-Verschlüsselung übertragen.
3. PC Share Mode (PC-Freigabemodus): Bestimmt den globalen gleichzeitigen KVM-Remotezugriff und ermöglicht bis zu acht Remotebenutzern die gleichzeitige Anmeldung bei einer LX-Einheit sowie die gleichzeitige Anzeige und Steuerung desselben Zielservers über das Gerät. Klicken Sie auf die Dropdownliste, um eine der folgenden Optionen auszuwählen:
   - Private (Privat) – Keine PC-Freigabe. Dies ist der Standardmodus. Jeder Zielserver ist jeweils nur für einen Benutzer exklusiv zugänglich.
   - PC-Share (PC-Freigabe) – Bis zu acht Benutzer (Administratoren oder Nicht-Administratoren) können gleichzeitig auf KVM-Zielserver zugreifen. Jeder Remotebenutzer besitzt dieselbe Kontrolle über Tastatur und Maus. Beachten Sie jedoch, dass eine ungleichmäßige Steuerung auftritt, wenn ein Benutzer seine Tastatur- bzw. Mauseingabe nicht unterbricht.
4. Wählen Sie bei Bedarf den Modus "VM Share" (VM-Freigabe) aus. Diese Option steht nur zur Verfügung, wenn der PC-Freigabemodus aktiviert wurde. Wenn dieses Kontrollkästchen aktiviert ist, werden virtuelle Medien für mehrere Benutzer freigegeben, d. h. diese können gemeinsam auf dieselbe virtuelle Mediensitzung zugreifen. Standardmäßig ist dieses Kontrollkästchen deaktiviert.
5. Wählen Sie bei Bedarf den Modus "Local Device Reset" (Lokales Gerät zurücksetzen) aus. Diese Option legt fest, welche Maßnahmen ergriffen werden, wenn die Taste zum Zurücksetzen der Hardware auf der Rückseite des Geräts gedrückt wird. Weitere Informationen finden Sie unter ***Zurücksetzen von LX mithilfe der Taste "Reset" (Zurücksetzen)*** (siehe "***Zurücksetzen des LX mithilfe der Taste "Reset" (Zurücksetzen)***" auf Seite 215). Wählen Sie eine der folgenden Optionen aus:

Modus zum Zurücksetzen eines lokalen Geräts	Beschreibung
Enable Local Factory Reset (Lokale Werkrücksetzung aktivieren, Standardeinstellung)	Setzt das LX-Gerät auf die werksseitigen Standardeinstellungen zurück.
Enable Local Admin Password Reset (Lokale	Setzt nur das Kennwort des lokalen Administrators zurück. Das Kennwort wird auf



Modus zum Zurücksetzen eines lokalen Geräts	Beschreibung
Administrator-Kennwortrücksetzung aktivieren)	"raritan" zurückgesetzt.
Disable All Local Resets (Alle lokalen Rücksetzungen deaktivieren)	Es wird keine Rücksetzungsmaßnahme ergriffen.

Prüfen Ihres Browsers auf AES-Verschlüsselung

LX unterstützt AES-256. Falls Sie wissen möchten, ob Ihr Browser AES verwendet, erkundigen Sie sich beim Hersteller, oder navigieren Sie mithilfe des Browsers und der zu prüfenden Verschlüsselungsmethode zu folgender Website: https://www.fortify.net/sslcheck.html. Diese Website erkennt die Verschlüsselungsmethode Ihres Browsers und zeigt einen entsprechenden Bericht an.

Hinweis: Die AES-128-Bit- oder -256-Bit-Verschlüsselung wird vom Internet Explorer® 6 nicht unterstützt.

Voraussetzungen und unterstützte Konfigurationen für die AES-256-Bit-Verschlüsselung

Die AES-256-Bit-Verschlüsselung wird nur von folgenden Webbrowsern unterstützt:

- Firefox® 2.0.0.x und 3.0 x (und höher)
- Internet Explorer 7 und 8

Für die AES-256-Bit-Verschlüsselung müssen außerdem die Sicherheitsrichtliniendateien für eine unbeschränkte Schlüssellänge der Java™ Cryptography Extension® (JCE®) installiert werden.

Diese sogenannten "Unlimited Strength Jurisdiction Policy Files" der verschiedenen JRE™-Versionen finden Sie unter folgendem Link im Bereich "Other Downloads" (Weitere Downloads):

- JRE1.6 - http://java.sun.com/javase/downloads/index_jdk5.jsp



SSL-Zertifikate

Das SSL-Protokoll (Secure Socket Layer) wird für den gesamten verschlüsselten Netzwerkdatenverkehr zwischen LX und einem mit der Einheit verbundenen Client verwendet. Wenn eine Verbindung hergestellt wird, muss sich LX gegenüber einem Client, der ein kryptografisches Zertifikat verwendet, identifizieren.

Es kann eine Zertifikatsregistrierungsanforderung (Certificate Signing Request, CSR) erzeugt und ein von der Zertifizierungsstelle (Certificate Authority, CA) signiertes Zertifikat auf dem LX-Gerät installiert werden. Die CA prüft die Identität des Absenders der CSR. Anschließend sendet die CA ein signiertes Zertifikat an den Absender. Das Zertifikat mit der Signatur der renommierten CA wird verwendet, um für die Identität des Zertifikatsinhabers zu bürgen.

Hinweis: Die CSR muss auf LX generiert werden.

So erstellen und installieren Sie ein SSL-Zertifikat:

1. Wählen Sie "Security" > "SSL Certificate" (Sicherheit > SSL-Zertifikat) aus.
2. Füllen Sie die folgenden Felder aus:
   a. "Common Name" (Allgemeiner Name) – Der Netzwerkname der LX-Einheit, wenn diese im Benutzernetzwerk installiert wurde (normalerweise der vollqualifizierte Domainname). Dieser ist mit dem Namen identisch, der für den Zugriff auf LX über einen Webbrowser verwendet wird, allerdings ohne das Präfix "http://". Sollte der hier angegebene Name nicht dem tatsächlichen Netzwerknamen entsprechen, wird im Browser eine Sicherheitswarnung angezeigt, wenn über HTTPS auf LX zugegriffen wird.
   b. "Organizational Unit" (Organisationseinheit) – In diesem Feld wird angegeben, zu welcher Abteilung der Organisation das LX-Gerät gehört.
   c. "Organization" (Organisation) – Der Name der Organisation, zu der das LX-Gerät gehört.
   d. "Locality/City" (Lokalität/Stadt) – Die Stadt, in der sich die Organisation befindet.
   e. "State/Province" (Bundesland/Region) – Das Bundesland oder die Region, in dem/der sich die Organisation befindet.
   f. "Country (ISO code)" [Land (ISO-Code)] – Das Land, in dem sich die Organisation befindet. Der ISO-Code ist der aus zwei Buchstaben bestehende Code der Internationalen Organisation für Normung, z. B. "DE" für Deutschland oder "US" für die USA.



g. "Challenge Password" (Challenge-Kennwort) – Einige Zertifizierungsstellen verlangen ein Challenge-Kennwort für die Authentifizierung von späteren Änderungen des Zertifikats (z. B. Widerruf des Zertifikats). Die Mindestlänge dieses Kennworts beträgt vier Zeichen.

h. "Confirm Challenge Password" (Challenge-Kennwort bestätigen) – Bestätigung des Challenge-Kennworts.

i. "Email" (E-Mail) – Die E-Mail-Adresse einer Kontaktperson, die für LX und dessen Sicherheit verantwortlich ist.

j. "Key Length" (Schlüssellänge) – Die Länge des erzeugten Schlüssels in Bits. Die Standardlänge ist 1024.

k. Aktivieren Sie das Kontrollkästchen "Create a Self-Signed Certificate" (Selbst signiertes Zertifikat erstellen) (falls zutreffend).

3. Klicken Sie auf "Create" (Erstellen), um die Zertifikatsregistrierungsanforderung (Certificate Signing Request, CSR) zu erzeugen.

▸ So laden Sie ein CSR-Zertifikat herunter:

1. Sie können die CSR und die Datei, die den bei der Erzeugung verwendeten privaten Schlüssel enthalten, herunterladen, indem Sie auf die Schaltfläche "Download" (Herunterladen) klicken.

Hinweis: Die CSR und die Datei für den privaten Schlüssel gehören zusammen und sollten auch dementsprechend verwendet werden. Wenn das signierte Zertifikat nicht mit dem bei der Erzeugung der ursprünglichen CSR verwendeten privaten Schlüssel übereinstimmt, kann das Zertifikat nicht verwendet werden. Dies gilt für das Hoch- und Herunterladen der CSR und den Dateien für den privaten Schlüssel.

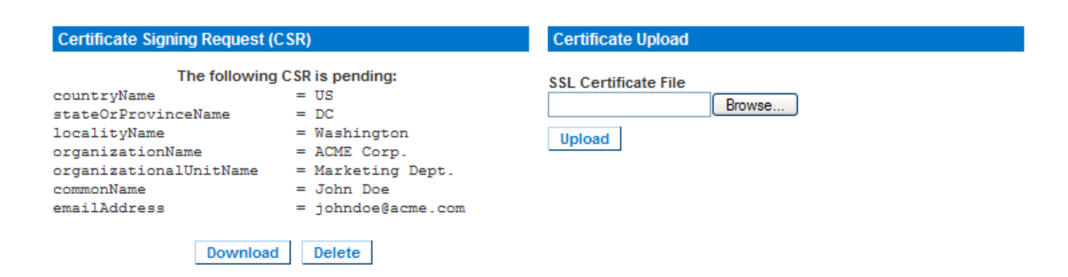
---

2. Senden Sie die gespeicherte CSR zur Zertifizierung an eine Zertifizierungsstelle. Sie erhalten von dieser das neue Zertifikat.

▸ So laden Sie eine CSR hoch:

1. Laden Sie das Zertifikat für LX hoch, indem Sie auf die Schaltfläche "Upload" (Hochladen) klicken.

Hinweis: Die CSR und die Datei für den privaten Schlüssel gehören zusammen und sollten auch dementsprechend verwendet werden. Wenn das signierte Zertifikat nicht mit dem bei der Erzeugung der ursprünglichen CSR verwendeten privaten Schlüssel übereinstimmt, kann das Zertifikat nicht verwendet werden. Dies gilt für das Hoch- und Herunterladen der CSR und den Dateien für den privaten Schlüssel.



Nach Abschluss dieser drei Schritte verfügt LX über ein eigenes Zertifikat zur Identifizierung gegenüber den Clients.

Wichtig: Wenn Sie die CSR auf der LX-Einheit löschen, kann diese nicht wiederhergestellt werden. Wenn Sie sie versehentlich gelöscht haben, müssen Sie die drei oben beschriebenen Schritte erneut durchführen. Um dies zu vermeiden, verwenden Sie die Downloadfunktion, sodass Sie über eine Kopie der CSR und des privaten Schlüssels verfügen.



Kapitel 8 Wartung

In diesem Kapitel

Audit Log (Prüfprotokoll)

Alle LX-Systemereignisse werden protokolliert. Das Prüfprotokoll kann bis zu 2 K Daten speichern, bevor die ältesten Einträge überschrieben werden. Zur Vermeidung des Verlusts von Prüfprotokolldaten exportieren Sie die Daten an einen Syslog-Server oder SNMP Manager. Konfigurieren Sie den Syslog-Server oder SNMP-Manager auf der Seite "Device Settings" (Geräteeinstellungen) > "Event Management" (Ereignisverwaltung). Informationen darüber, welche Daten im Prüfprotokoll und im Syslog erfasst werden, finden Sie unter ***Im Prüfprotokoll und im Syslog erfasste Ereignisse*** (auf Seite 238).

So zeigen Sie das Prüfprotokoll für Ihre LX-Einheit an:

1. Wählen Sie **Maintenance > Audit Log** (Wartung > Prüfprotokoll). Die Seite "Audit Log" (Prüfprotokoll) wird angezeigt.

   Die Seite "Audit Log" (Prüfprotokoll) enthält Ereignisse sortiert nach Datum und Uhrzeit, wobei die letzten Ereignisse zuerst aufgeführt werden. Das Prüfprotokoll enthält die folgenden Informationen:

   - Date (Datum) – Datum und Uhrzeit des Ereignisses, basierend auf dem 24-h-Zeitformat.
   - Event (Ereignis) – Der Ereignisname, wie er auf der Seite "Event Management" (Ereignisverwaltung) aufgeführt wird.
   - Description (Beschreibung) – Detaillierte Beschreibung des Ereignisses.

So speichern Sie das Prüfprotokoll:

Hinweis: Sie können das Prüfprotokoll nur mithilfe der LX-Remotekonsole speichern, nicht jedoch mit der lokalen Konsole.

1. Klicken Sie auf "Save to File" (Speichern unter). Ein Dialogfeld zum Speichern der Datei wird angezeigt.

2. Wählen Sie einen Dateinamen und Speicherort aus, und klicken Sie auf "Save" (Speichern). Das Prüfprotokoll wird mit dem festgelegten Namen lokal am ausgewählten Ort auf dem Client-Computer gespeichert.

So blättern Sie durch das Prüfprotokoll:

- Verwenden Sie die Links **[Older]** ([Älter]) und **[Newer]** ([Neuer]).



"Device Information" (Geräteinformationen)

Die Seite "Device Information" (Geräteinformationen) enthält detaillierte Angaben zu Ihrem LX-Gerät und den verwendeten CIMs. Diese Informationen benötigen Sie, wenn Sie sich mit dem technischen Kundendienst von Raritan in Verbindung setzen.

So zeigen Sie Informationen zu Ihrer LX-Einheit und den CIMs an:

- Wählen Sie "Maintenance > Device Information" (Wartung > Geräteinformationen). Die Seite "Device Information" (Geräteinformationen) wird angezeigt.

Zu der LX-Einheit werden folgende Informationen angezeigt:

- Model (Modell)
- Hardware Revision (Hardware-Revision)
- Firmware Version (Firmware-Version)
- Serial Number (Seriennummer)
- MAC Address (MAC-Adresse)

Zu den verwendeten CIMs werden folgende Informationen angezeigt:

- "Port (Number)" [Port (Nummer)]
- Name
- CIM-Typ – DCIM oder VM
- Firmware Version (Firmware-Version)
- "Serial Number of the CIM" (Seriennummer des CIM) – Diese Nummer wird direkt aus dem CIM abgerufen.

Hinweis: Nur der numerische Teil bzw. die Seriennummern werden für DCIM-USB, DCIM-PS2 und DCIM-USB G2 CIMs angezeigt. Es wird beispielsweise XXX1234567 angezeigt. Das Präfix GN der Seriennummer wird für CIMs angezeigt, deren Seriennummern in Feldern konfiguriert wurden.

Device Information

Model:	DLX-116
Hardware Revision:	0x10
Firmware Version:	2.4.5.1.79
Serial Number:	HKK1600002
MAC Address:	00:0d:5d:00:01:96

CIM Information

▲ Port	Name	Type	Firmware Version	Serial Number
4	FC15	Dual-VM	3A88	GN000D5D01339E3C3D3F6D70666936
8	FC11	Dual-VM	3A88	PQ21010199
13	Dominion_LX_Port13	MCUTP	N/A	N/A
16	DominionLX	Dual-VM	3A88	PQ28450291



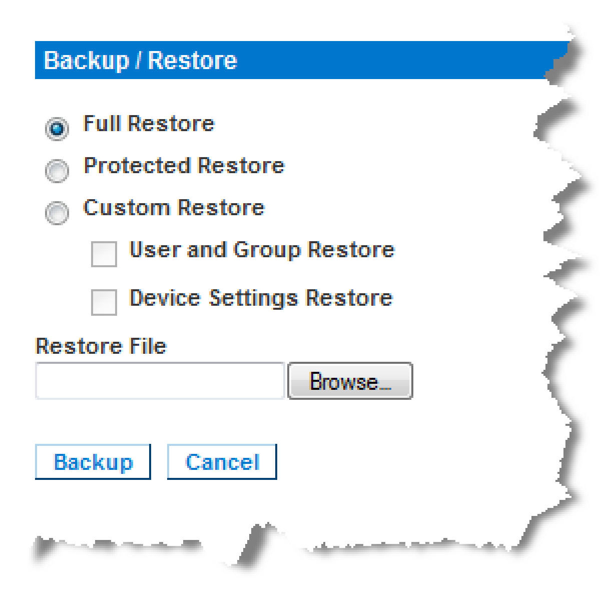
"Backup/Restore" (Sicherung/Wiederherstellung)

Auf der Seite "Backup/Restore" (Sicherung/Wiederherstellung) können Sie die Einstellungen und die Konfiguration der LX-Einheit sichern und wiederherstellen.

Dieses Feature dient nicht nur der Gewährleistung der Geschäftskontinuität, sondern Sie können damit auch viel Zeit sparen. So können Sie Ihrem Team beispielsweise schnell von einer anderen LX-Einheit aus Zugriff gewähren, indem Sie die Benutzerkonfigurationseinstellungen des verwendeten LX-Geräts sichern und auf dem neuen LX-Gerät wiederherstellen. Sie können auch eine LX-Einheit einrichten und deren Konfiguration auf mehrere andere LX-Geräte kopieren.

► So greifen Sie auf die Seite "Backup/Restore" (Sicherung/Wiederherstellung) zu:

- Wählen Sie "Maintenance > Backup/Restore" (Wartung > Sicherung/Wiederherstellung). Die Seite "Backup/Restore" (Sicherung/Wiederherstellung) wird angezeigt.



Hinweis: Es wird immer das komplette System gesichert. Bei der Wiederherstellung können Sie zwischen einer vollständigen und einer teilweisen Wiederherstellung wählen.

► Wenn Sie Firefox® oder Internet Explorer® 5 (oder älter) zur Sicherung Ihres LX verwenden:

1. Klicken Sie auf "Backup" (Sichern). Das Dialogfeld "File Download" (Datei-Download) wird angezeigt.

2. Klicken Sie auf "Save" (Speichern). Das Dialogfeld "Save As" (Speichern unter) wird angezeigt.
3. Wählen Sie einen Speicherort aus, geben Sie einen Dateinamen an, und klicken Sie auf "Save" (Speichern). Das Dialogfeld "Download Complete" (Download abgeschlossen) wird angezeigt.
4. Klicken Sie auf "Close" (Schließen). Die Sicherungsdatei wird unter dem festgelegten Namen lokal am ausgewählten Ort auf dem Client-Computer gespeichert.

▶ Wenn Sie Internet Explorer 6 (oder höher) zur Sicherung Ihres LX verwenden:

1. Klicken Sie auf "Backup" (Sichern). Das Dialogfeld "File Download" (Dateidownload) mit der Schaltfläche "Open" (Öffnen) wird angezeigt. Klicken Sie nicht auf "Open" (Öffnen).

   Bei Internet Explorer 6 (und höher) wird Internet Explorer als Standardanwendung zum Öffnen von Dateien verwendet. Sie werden aufgefordert, die Datei zu öffnen oder sie zu speichern. Um dies zu verhindern, müssen Sie eine Änderung vornehmen, sodass WordPad® als Standardanwendung zum Öffnen von Dateien verwendet wird.

2. Dies funktioniert wie folgt:
   a. Speichern Sie die Sicherungsdatei. Die Sicherungsdatei wird unter dem festgelegten Namen lokal am ausgewählten Ort auf dem Client-Computer gespeichert.
   b. Ist die Datei gespeichert, navigieren Sie zu dieser und klicken mit der rechten Maustaste darauf. Klicken Sie im dem Kontextmenü auf "Eigenschaften".
   c. Klicken Sie auf der Registerkarte "Allgemein" auf die Schaltfläche "Ändern", und wählen Sie im angezeigten Dialogfeld "WordPad" aus.



▶ So stellen Sie die LX-Einheit wieder her:

WARNUNG: Gehen Sie bei der Wiederherstellung Ihrer LX-Einheit auf eine frühere Version vorsichtig vor. Die bei der Sicherung gespeicherten Benutzernamen und Kennwörter werden wiederhergestellt. Wenn Sie sich nicht mehr an die alten Anmeldedaten für den Administrator erinnern können, wird Ihnen der Zugriff auf die LX-Einheit verweigert.

Falls Sie zum Zeitpunkt der Sicherung eine andere IP-Adresse verwendet haben, wird auch diese wiederhergestellt. Wenn Sie DHCP konfiguriert haben, sollten Sie diesen Vorgang nur ausführen, wenn Sie Zugriff auf den lokalen Port haben, um nach der Aktualisierung die IP-Adresse zu prüfen.

1. Wählen Sie eine Wiederherstellungsart aus:
   - "Full Restore" (Vollständige Wiederherstellung) – Das gesamte System wird wiederhergestellt. Wird normalerweise für herkömmliche Sicherungs- und Wiederherstellungszwecke verwendet.
   - "Protected Restore" (Geschützte Wiederherstellung) – Alle Daten werden wiederhergestellt, mit Ausnahme von gerätespezifischen Informationen wie IP-Adresse, Name usw. Mit dieser Option können Sie eine LX-Einheit einrichten und deren Konfiguration auf mehrere andere LX-Geräte kopieren.
   - "Custom Restore" (Benutzerdefinierte Wiederherstellung) – Bei dieser Option stehen Ihnen die Kontrollkästchen "User and Group Restore" (Wiederherstellung von Benutzern und Gruppen) und "Device Settings Restore" (Wiederherstellung der Geräteeinstellungen) zur Auswahl zur Verfügung.
     - "User and Group Restore" (Wiederherstellung von Benutzern und Gruppen) – Diese Option umfasst nur Benutzer- und Gruppeninformationen. Bei dieser Option werden das Zertifikat und die Dateien für den privaten Schlüssel *nicht* wiederhergestellt. Verwenden Sie sie, um schnell Benutzer auf einem anderen LX-Gerät einzurichten.
     - "Device Settings Restore" (Wiederherstellung der Geräteeinstellungen) – Verwenden Sie diese Option, um schnell die Geräteinformationen zu kopieren.
2. Klicken Sie auf "Browse" (Durchsuchen). Das Dialogfeld "Choose file" (Datei auswählen) wird angezeigt.
3. Navigieren Sie zur gewünschten Sicherungsdatei, markieren Sie sie, und klicken Sie auf "Open" (Öffnen). Die ausgewählte Datei wird im Feld "Restore File" (Datei wiederherstellen) aufgeführt.
4. Klicken Sie auf "Restore" (Wiederherstellen). Die Konfiguration wird basierend auf der gewählten Wiederherstellungsart wiederhergestellt.

Aktualisieren von CIMs

Gehen Sie wie unten beschrieben vor, um CIMs mithilfe der im Speicher des LX-Geräts abgelegten Firmwareversionen zu aktualisieren. Im Allgemeinen werden alle CIMs aktualisiert, wenn Sie die Gerätefirmware über die Seite Firmware Upgrade (Firmwareaktualisierung) aktualisieren.

Hinweis: Nur D2CIM-VUSB und D2CIM-DVUSB können auf dieser Seite aktualisiert werden.

So aktualisieren Sie CIMs mithilfe des LX-Speichers:

1. Wählen Sie "Maintenance" > "CIM Firmware Upgrade" (Wartung > CIM-Firmwareaktualisierung) aus. Die Seite "CIM Firmware Upgrade" (CIM-Firmwareaktualisierung) wird geöffnet.

   Sie erkennen die CIMs leicht an den Angaben in den Feldern "Port", "Name", "Type" (Typ), "Current CIM Version" (Aktuelle CIM-Version) und "Upgrade CIM Version" (Neue CIM-Version).

2. Aktivieren Sie für alle CIMs, die aktualisiert werden sollen, das Kontrollkästchen "Selected" (Ausgewählt).
3. Klicken Sie auf "Upgrade" (Aktualisieren). Sie werden aufgefordert, die Aktualisierung zu bestätigen.
4. Klicken Sie auf OK, um fortzufahren. Während des Vorgangs werden Statusleisten angezeigt. Die Aktualisierung dauert maximal zwei Minuten pro CIM.

Aktualisieren der Firmware

Auf der Seite "Firmware Upgrade" (Firmwareaktualisierung) können Sie die Firmware von LX und allen damit verbundenen CIMs aktualisieren. Diese Seite ist nur in der LX-Remote-Konsole verfügbar.

Wichtig: Schalten Sie während der Aktualisierung die LX-Einheit nicht aus und trennen Sie nicht die Verbindung zu den CIMs, da dies zu Schäden an der Einheit bzw. den CIMs führen könnte.

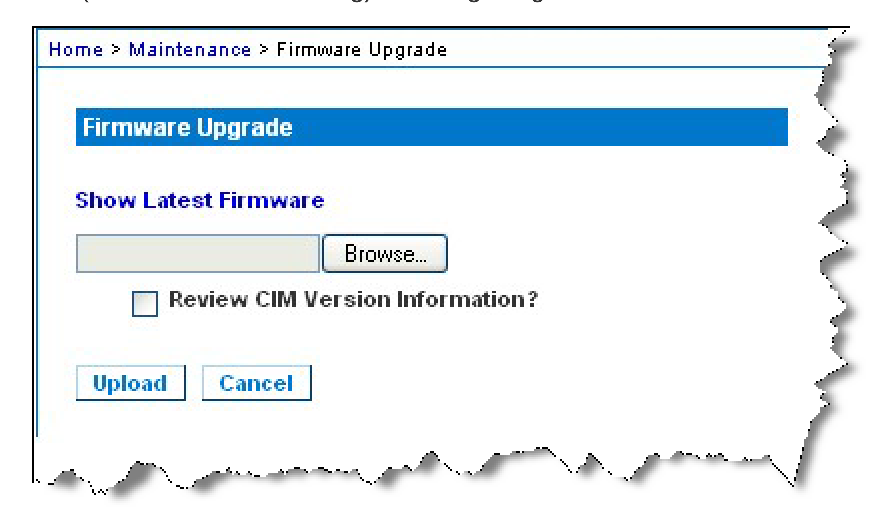
So aktualisieren Sie die LX-Einheit:

1. Suchen Sie die entsprechende Raritan-Firmwaredistributionsdatei (*.RFP) auf der Seite für Firmwareaktualisierungen der ***Raritan-Website http://www.raritan.com***.
2. Entpacken Sie die Datei. Lesen Sie alle Anweisungen in den Firmware-ZIP-Dateien sorgfältig durch, bevor Sie die Aktualisierung durchführen.



Hinweis: Kopieren Sie die Firmware-Aktualisierungsdatei vor dem Hochladen auf einen lokalen PC. Laden Sie die Datei nicht von einem Netzwerklaufwerk.

3. Wählen Sie "Maintenance > Firmware Upgrade" (Wartung > Firmware-Aktualisierung). Die Seite "Firmware Upgrade" (Firmwareaktualisierung) wird angezeigt.



4. Klicken Sie auf die Schaltfläche "Browse" (Durchsuchen), um zu dem Verzeichnis zu navigieren, in dem Sie die Aktualisierungsdatei entpackt haben.
5. Aktivieren Sie das Kontrollkästchen "Review CIM Version Information?" (CIM-Versionsinformationen überprüfen?), wenn Informationen zu den Versionen der verwendeten CIMs angezeigt werden sollen.
6. Klicken Sie auf der Seite "Firmware Upgrade" (Firmware-Aktualisierung) auf "Upload" (Hochladen). Ihnen werden Informationen zur Aktualisierung und den Versionsnummern sowie zu den CIMs (falls Sie das entsprechende Kontrollkästchen aktiviert haben) angezeigt.

Hinweis: Zu diesem Zeitpunkt werden verbundene Benutzer abgemeldet, und neue Anmeldeversuche werden blockiert.

7. Klicken Sie auf "Upgrade" (Aktualisieren). Warten Sie, bis der Vorgang abgeschlossen ist. Während des Vorgangs werden Statusinformationen und Fortschrittsleisten angezeigt. Nach Abschluss der Aktualisierung wird die Einheit neu gestartet (ein Tonsignal zeigt an, dass der Neustart abgeschlossen ist).

Schließen Sie den Browser, wenn Sie dazu aufgefordert werden, und warten Sie ungefähr fünf Minuten, bevor Sie sich erneut bei der LX-Einheit anmelden.

Informationen zur Aktualisierung der Gerätefirmware mithilfe des Multi-Platform-Clients finden Sie im Abschnitt **Aktualisieren der Gerätefirmware** im Benutzerhandbuch **KVM and Serial Access Clients Guide**.

Hinweis: Firmwareaktualisierungen über Modem werden nicht unterstützt.

Upgrade History (Aktualisierungsverlauf)

LX liefert Informationen über die Aktualisierungen, die auf LX und den angeschlossenen CIMs durchgeführt wurden.

So zeigen Sie den Aktualisierungsverlauf an:

- Wählen Sie "Maintenance > Upgrade History" (Wartung > Aktualisierungsverlauf). Die Seite "Upgrade History" (Aktualisierungsverlauf) wird angezeigt.

Es werden Informationen zu den ausgeführten LX-Aktualisierungen, dem Endstatus der Aktualisierung, den Start- und Abschlusszeiten sowie den vorherigen und aktuellen Firmwareversionen angezeigt. Es werden außerdem Informationen zu den CIMs bereitgestellt. Diese können angezeigt werden, indem Sie auf den Link der entsprechenden Aktualisierung klicken. Die folgenden CIM-Informationen stehen zur Verfügung:

- "Type" (Typ) – Der CIM-Typ
- "Port" (Port) – Der Port, an dem das CIM angeschlossen ist
- "User" (Benutzer) – Der Benutzer, der die Aktualisierung durchgeführt hat
- "IP" (IP) – IP-Adresse der Firmware
- "Start Time" (Startzeit) – Startzeit der Aktualisierung
- "End Time" (Abschlusszeit) – Abschlusszeit der Aktualisierung
- "Previous Version" (Vorherige Version) – Vorherige CIM-Firmwareversion
- "Upgrade Version" (Neue Version) – Aktuelle CIM-Firmwareversion
- "CIMs" (CIMs) – Aktualisierte CIMs
- "Result" (Ergebnis) – Das Ergebnis der Aktualisierung (erfolgreich oder fehlgeschlagen)



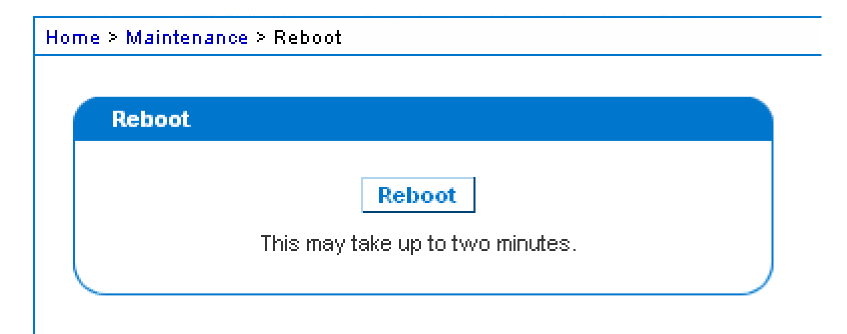
Neustart der LX-Einheit

Auf der Seite "Reboot" (Neustart) können Sie LX auf sichere und kontrollierte Weise neustarten. Dies ist die empfohlene Methode zum Neustarten.

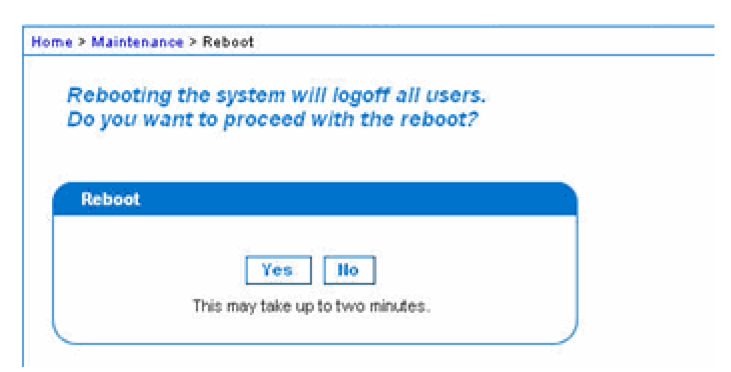
Wichtig: Alle seriellen und KVM-Verbindungen werden getrennt und alle Benutzer abgemeldet.

So starten Sie die LX-Einheit neu:

1. Wählen Sie **Maintenance > Reboot** (Wartung > Neustart). Die Seite **Reboot** (Neustart) wird angezeigt.



2. Klicken Sie auf "Reboot" (Neustart). Sie werden aufgefordert, die Aktion zu bestätigen. Klicken Sie auf "Yes" (Ja), um fortzufahren.



Kapitel 9 Diagnostics (Diagnose)

In diesem Kapitel

Network Interface (Netzwerkschnittstelle)

LX liefert Informationen zum Status der Netzwerkschnittstelle.

So zeigen Sie Informationen zur Netzwerkschnittstelle an:

- Wählen Sie "Diagnostics > Network Interface" (Diagnose > Netzwerkschnittstelle). Die Seite "Network Interface" (Netzwerkschnittstelle) wird angezeigt.

Diese Seite enthält die folgenden Informationen:

- Funktionsfähigkeit der Ethernet-Schnittstelle
- Erreichbarkeit des Gateways
- Derzeit aktiver LAN-Port

So aktualisieren Sie diese Informationen:

- Klicken Sie auf "Refresh" (Aktualisieren).

Network Interface

Refresh

Result:

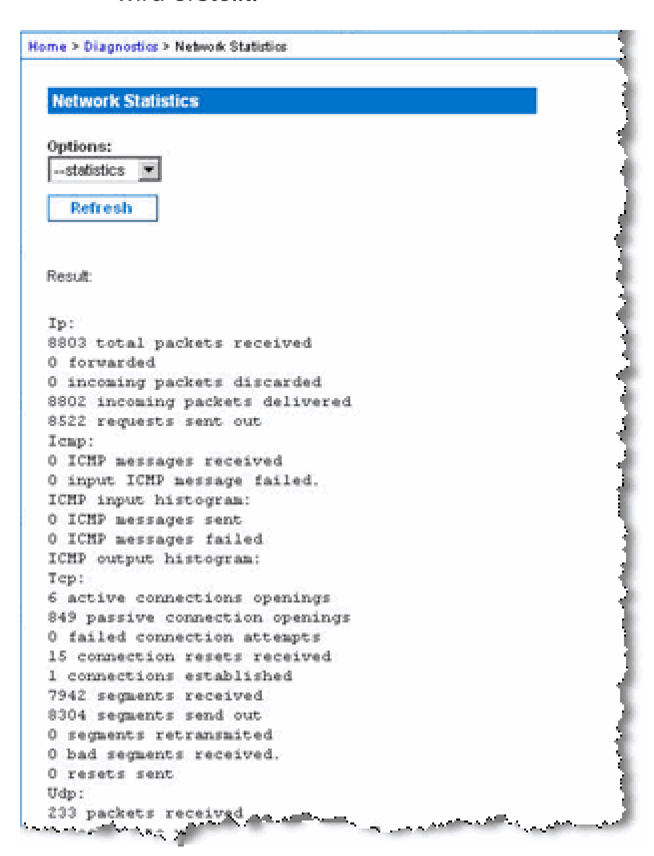
```
Link state: autonegotiation on, 100 Mbps, full duplex, link ok
eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
link/ether 00:0d:5d:ca:b1:f8 brd ff:ff:ff:ff:ff:ff
inet 192.168.51.101/24 brd 192.168.51.255 scope global eth0
LAN 1 is active.
```

Network Statistics (Netzwerkstatistik)

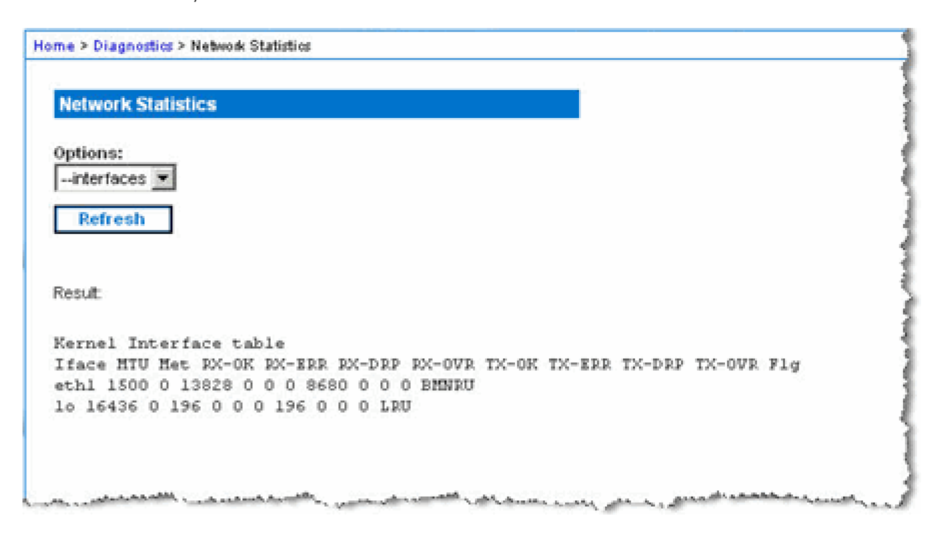
LX liefert Statistiken über die Netzwerkschnittstelle.

So zeigen Sie Statistiken über die Netzwerkschnittstelle an:

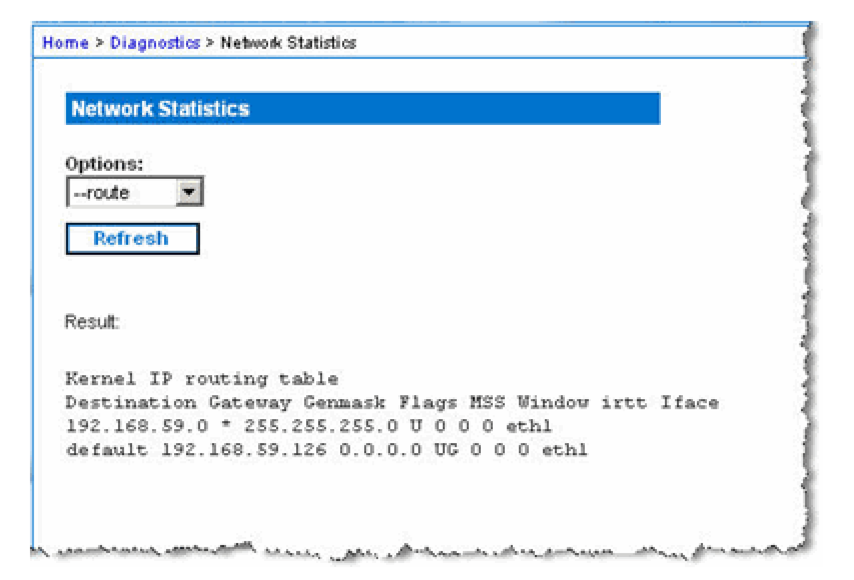
1. Wählen Sie **Diagnostics > Network Statistics** (Diagnose > Netzwerkstatistik). Die Seite **Network Statistics** (Netzwerkstatistik) wird angezeigt.
2. Wählen Sie eine Option aus der Dropdown-Liste **Options**:
   - Statistics (Statistiken) – Eine Seite, die der hier gezeigten ähnelt, wird erstellt.



- Interfaces (Schnittstellen) – Eine Seite, die der hier gezeigten ähnelt, wird erstellt.



- Route – Eine Seite, die der hier gezeigten ähnelt, wird erstellt.



3. Klicken Sie auf "Refresh" (Aktualisieren). Die entsprechenden Informationen werden im Feld "Result" (Ergebnis) angezeigt.

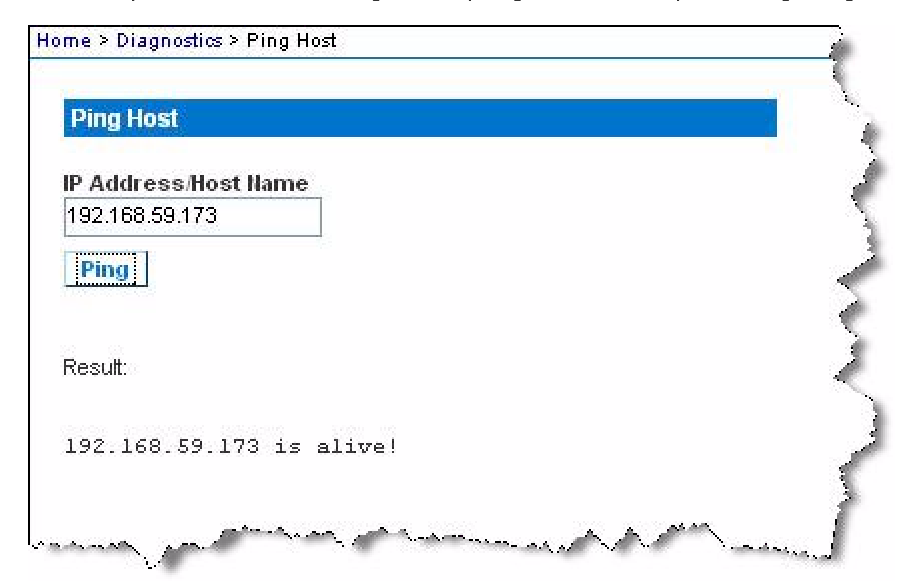


Ping Host (Ping an den Host)

Ping ist ein Netzwerktool, mit dem getestet werden kann, ob ein bestimmter Host oder eine IP-Adresse über ein IP-Netzwerk erreichbar ist. Mithilfe der Seite "Ping Host" (Ping an den Host) können Sie herausfinden, ob ein Zielserver oder eine andere LX-Einheit erreichbar ist.

► **So senden Sie ein Ping an den Host:**

1. Wählen Sie "Diagnostics" > "Ping Host" (Diagnose > Ping an den Host) aus. Die Seite "Ping Host" (Ping an den Host) wird angezeigt.



2. Geben Sie entweder den Hostnamen oder die IP-Adresse im Feld "IP Address/Host Name" (IP-Adresse/Hostname) ein.

Hinweis: Der Hostname darf aus maximal 232 Zeichen bestehen.

3. Klicken Sie auf "Ping". Die Ping-Ergebnisse werden im Feld "Result" (Ergebnis) angezeigt.

Trace Route to Host (Route zum Host zurückverfolgen)

Die Routenverfolgung ist ein Netzwerktool, mit dem Sie die Route bis zum angegebenen Hostnamen oder der IP-Adresse zurückverfolgen können.

► **So verfolgen Sie die Route bis zum Host zurück:**

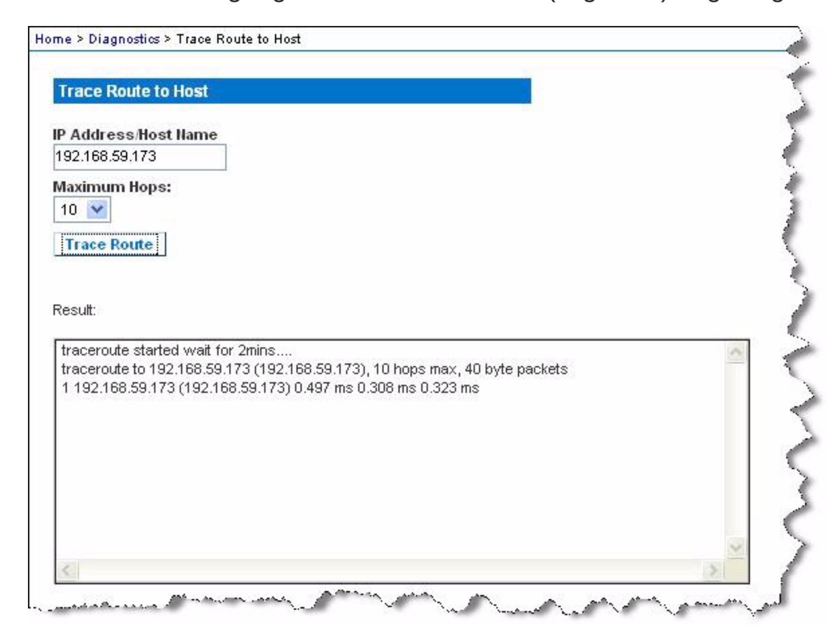
1. Wählen Sie **Diagnostics > Trace Route to Host** (Diagnose > Route zum Host zurückverfolgen). Die Seite **Trace Route to Host** (Route zum Host zurückverfolgen) wird angezeigt.

2. Geben Sie entweder die IP-Adresse oder den Hostnamen im Feld "IP Address/Host Name" (IP-Adresse/Hostname) ein.

Hinweis: Der Hostname darf aus maximal 232 Zeichen bestehen.

---

3. Wählen Sie in der Dropdownliste "Maximum Hops" (Maximale Teilstrecken) eine Option aus (5 bis 50 in Schritten von 5).
4. Klicken Sie auf "Trace Route" (Route zurückverfolgen). Der Befehl wird für den angegebenen Hostnamen oder die IP-Adresse sowie die maximale Zahl der Teilstrecken ausgeführt. Das Ergebnis der Routenverfolgung wird im Feld "Result" (Ergebnis) angezeigt.





Device Diagnostics (Gerätediagnose)

Hinweis: Diese Seite ist für die Außendienstmitarbeiter von Raritan gedacht. Verwenden Sie sie nur unter Anleitung des technischen Kundendienstes.

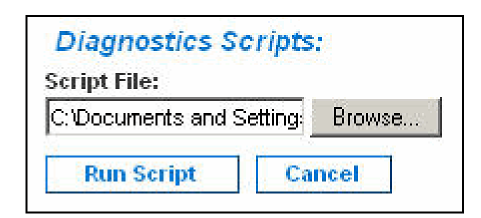
Auf der Seite "Device Diagnostics" (Gerätediagnose) werden die Diagnoseinformationen von LX auf den Client-PC heruntergeladen. Auf dieser Seite haben Sie zwei Möglichkeiten:

- Führen Sie während einer Sitzung zum Debuggen eines schwerwiegenden Fehlers ein vom technischen Kundendienst von Raritan bereitgestelltes Spezialdiagnoseskript aus. Das Skript wird auf das Gerät hochgeladen und ausgeführt. Nachdem das Skript ausgeführt wurde, können Sie die Diagnosemeldungen mithilfe der Funktion "Save to File" (Speichern unter) herunterladen.
- Laden Sie das Protokoll der Gerätediagnose vom LX-Gerät auf den Client herunter, um eine Übersicht der Diagnosemeldungen zu erhalten. Diese verschlüsselte Datei wird anschließend an den technischen Kundendienst von Raritan gesendet. Nur Raritan kann diese Datei interpretieren.

Hinweis: Auf diese Seite können nur Benutzer mit Administratorrechten zugreifen.

So führen Sie die LX-Systemdiagnose aus:

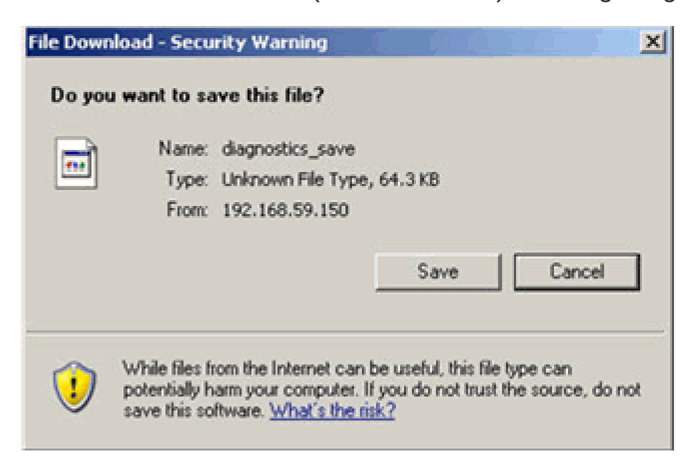
1. Wählen Sie "Diagnostics" > "LX Diagnostics" (Diagnose > LX-Diagnose) aus. Die LX-Diagnoseseite wird angezeigt.
2. So führen Sie eine Diagnoseskriptdatei aus, die Sie per E-Mail vom technischen Kundendienst von Raritan erhalten haben:
   a. Rufen Sie die Diagnosedatei von Raritan ab, und entpacken Sie sie gegebenenfalls.
   b. Klicken Sie auf "Browse" (Durchsuchen). Das Dialogfeld "Choose File" (Datei auswählen) wird angezeigt.
   c. Navigieren Sie zur gewünschten Diagnosedatei, und markieren Sie sie.
   d. Klicken Sie auf "Open" (Öffnen). Die Datei wird im Feld "Script File" (Skriptdatei) angezeigt.



e. Klicken Sie auf "Run Script" (Skript ausführen). Senden Sie diese Datei an den technischen Kundendienst von Raritan.

3. So erstellen Sie eine Diagnosedatei, die Sie an den technischen Kundendienst von Raritan senden können:

a. Klicken Sie auf "Save to File" (Speichern unter). Das Dialogfeld "File Download" (Dateidownload) wird angezeigt.



b. Klicken Sie auf "Save" (Speichern). Das Dialogfeld "Save As" (Speichern unter) wird angezeigt.

c. Navigieren Sie zum gewünschten Verzeichnis, und klicken Sie auf "Save" (Speichern).

d. Senden Sie diese Datei an die vom technischen Kundendienst von Raritan angegebene E-Mail-Adresse.



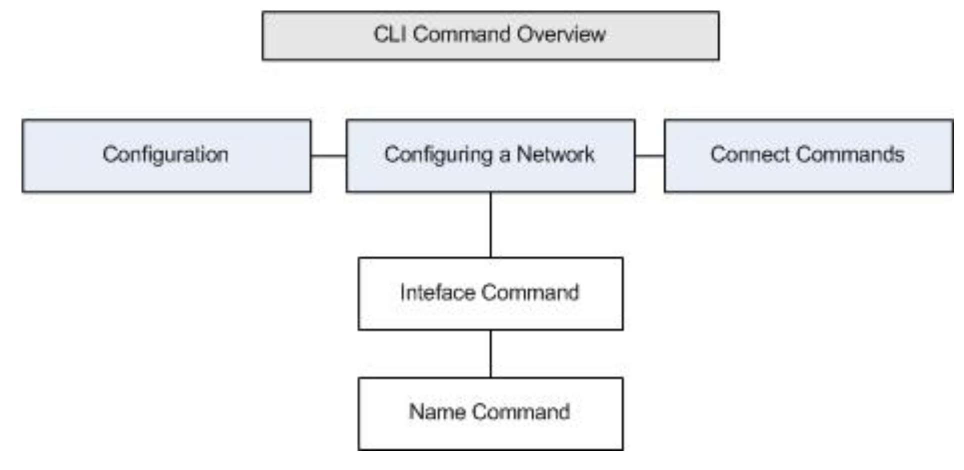
Kapitel 10 Kommandozeilenschnittstelle (CLI)

In diesem Kapitel

Überblick

Die Kommandozeilenschnittstelle (Command Line Interface, CLI) kann verwendet werden, um die LX-Netzwerkschnittstelle zu konfigurieren und Diagnosefunktionen durchzuführen, vorausgesetzt, Sie verfügen über die erforderlichen Berechtigungen.

Das folgenden Abbildungen bieten eine Übersicht über die Befehle der Kommandozeilenschnittstelle. Eine Liste der Befehle, einschließlich Definitionen und Verknüpfungen zu den Abschnitten in diesem Kapitel, die Beispiele für diese Befehle enthalten, finden Sie unter ***Befehle der Kommandozeilenschnittstelle*** (siehe "***Befehle der Befehlszeilenschnittstelle***" auf Seite 199).



Die folgenden allgemeinen Befehle können auf allen Ebenen der Befehlszeilenschnittstelle der Abbildung oben verwendet werden: "top", "history", "log off", "quit", "show" und "help"



Zugriff auf LX über die Kommandozeilenschnittstelle

Verwenden Sie eine der folgenden Methoden, um auf die LX-Einheit zuzugreifen:

- SSH (Secure Shell) über IP-Verbindung

Verschiedene SSH-Clients stehen hier zur Verfügung:

- Putty - ***http://www.chiark.greenend.org.uk/~sgtatham/putty/ http://www.chiark.greenend.org.uk/~sgtatham/putty/***
- SSH Client von ssh.com - ***www.ssh.com http://www.ssh.com***
- Applet SSH Client - ***www.netspace.org/ssh http://www.netspace.org/ssh***
- OpenSSH Client - ***www.openssh.org http://www.openssh.org***

SSH-Verbindung mit LX

Verwenden Sie zur Verbindung mit LX einen SSH-Client, der SSH V2 unterstützt. Sie müssen den SSH-Zugriff auf der Seite "Devices Services" (Gerätedienste) aktivieren.

Hinweis: Aus Sicherheitsgründen werden SSH-V1-Verbindungen von LX nicht unterstützt.

SSH-Zugriff über einen Windows-PC

So öffnen Sie eine SSH-Sitzung über einen Windows®-PC:

1. Starten Sie die SSH-Clientsoftware.
2. Geben Sie die IP-Adresse des LX-Servers ein. Beispielsweise 192.168.0.192.
3. Wählen Sie "SSH" aus (der standardmäßige Konfigurations-Port lautet 22).
4. Klicken Sie auf "Open" (Öffnen).

Die Eingabeaufforderung `login as:` (Anmelden als:) wird angezeigt.

Siehe ***Anmelden*** (auf Seite 195).



SSH-Zugriff über eine UNIX-/Linux-Workstation

Geben Sie den folgenden Befehl ein, um eine SSH-Sitzung über eine UNIX®-/Linux®-Workstation zu öffnen und sich als Admin-Benutzer anzumelden:

```
ssh -l admin 192.168.30.222
```

Die Eingabeaufforderung für das Kennwort wird angezeigt.

Siehe ***Anmelden*** (auf Seite 195).

Anmelden

Geben Sie zum Anmelden den Benutzernamen „admin“ wie gezeigt ein:

1. Melden Sie sich als `admin` an.
2. Die Eingabeaufforderung für das Kennwort wird angezeigt. Geben Sie das Standardkennwort ein: *raritan*

   Der Begrüßungsbildschirm wird angezeigt. Sie sind jetzt als Administrator angemeldet.

Wenn Sie den folgenden Abschnitt ***Navigation in der Kommandozeilenschnittstelle*** (auf Seite 195) gelesen haben, können Sie die Schritte zur Erstkonfiguration durchführen.

Navigation in der Kommandozeilenschnittstelle

Vor der Verwendung der Kommandozeilenschnittstelle sollten Sie sich mit der Navigation und Syntax in der Kommandozeilenschnittstelle vertraut machen. Es stehen Ihnen außerdem einige Tastenkombinationen zur Verfügung, mit denen die Verwendung der Kommandozeilenschnittstelle erleichtert wird.



Vervollständigen von Befehlen

Die Kommandozeilenschnittstelle unterstützt das Vervollständigen teilweise eingegebener Befehle. Drücken Sie die Tabulatortaste, wenn Sie die ersten Zeichen eines Eintrags eingegeben haben. Wenn die Zeichen mit einem Befehl eindeutig übereinstimmen, vervollständigt die Kommandozeilenschnittstelle den Eintrag.

- Wird keine Übereinstimmung gefunden, zeigt die Kommandozeilenschnittstelle die gültigen Einträge für die Ebene an.
- Wenn mehrere Übereinstimmungen gefunden werden, zeigt die Kommandozeilenschnittstelle alle gültigen Einträge an.

Geben Sie weiteren Text ein, damit eine eindeutige Übereinstimmung gefunden werden kann, und vervollständigen Sie den Eintrag mithilfe der Tabulatortaste.

Syntax der Kommandozeilenschnittstelle – Tipps und Zugriffstasten

Tipps

- Befehle werden in alphabetischer Reihenfolge aufgeführt.
- Bei Befehlen wird die Groß-/Kleinschreibung nicht beachtet.
- Parameternamen bestehen aus einem Wort ohne Unterstrich.
- Für Befehle ohne Argumente werden standardmäßig die aktuellen Einstellungen für den Befehl angezeigt.
- Wenn Sie nach dem Befehl ein Fragezeichen (?) eingeben, wird die Hilfe für diesen Befehl angezeigt.
- Ein senkrechter Strich (|) zeigt eine Auswahl im Bereich der optionalen oder erforderlichen Schlüsselwörter oder Argumente an.

Zugriffstasten

- Drücken Sie die Pfeil-nach-oben-Taste, um den letzten Eintrag anzuzeigen.
- Drücken Sie die Rücktaste, um das zuletzt eingegebene Zeichen zu löschen.
- Drücken Sie "Strg+C", um einen Befehl zu beenden oder abzubrechen, wenn Sie die falschen Parameter eingegeben haben.
- Drücken Sie die Eingabetaste, um den Befehl auszuführen.
- Drücken Sie die Tabulatortaste, um einen Befehl zu vervollständigen. Beispiel: `Admin Port > Conf.` Das System zeigt dann die Eingabeaufforderung `Admin Port > Config >` an.



Allgemeine Befehle für alle Ebenen der Kommandozeilenschnittstelle

Im Folgenden werden die Befehle aufgelistet, die auf allen Ebenen der Kommandozeilenschnittstelle verfügbar sind. Diese Befehle dienen auch zur Navigation in der Kommandozeilenschnittstelle.

Befehle	Beschreibung
top	Wechselt zur höchsten Ebene der Hierarchie der Kommandozeilenschnittstelle oder der Eingabeaufforderung "username" (Benutzername).
history	Zeigt die letzten 200 Befehle an, die der Benutzer in die Kommandozeilenschnittstelle von LX eingegeben hat.
help	Zeigt eine Übersicht der Syntax der Kommandozeilenschnittstelle an.
quit	Der Benutzer kehrt eine Ebene zurück.
logout	Beendet die Benutzersitzung.

Erstkonfiguration über die Kommandozeilenschnittstelle

Hinweis: Diese Schritte unter Verwendung der Kommandozeilenschnittstelle sind optional, da dieselbe Konfiguration auch über KVM erfolgen kann. Weitere Informationen finden Sie unter **Erste Schritte** *(auf Seite 13).*

LX-Geräte werden werksseitig mit Standardeinstellungen geliefert. Wenn Sie das Gerät zum ersten Mal einschalten und verbinden, müssen Sie die folgenden Grundparameter einstellen, sodass vom Netzwerk aus sicher auf das Gerät zugegriffen werden kann.

1. Kennwort des Administrators zurücksetzen. Alle LX-Geräte verfügen zunächst über dasselbe Standardkennwort. Um Sicherheitsverletzungen zu vermeiden, müssen Sie deshalb das Administratorkennwort "raritan" in ein benutzerdefiniertes Kennwort für Administratoren, die das LX-Gerät verwalten, ändern.
2. IP-Adresse, Subnetzmaske und Gateway-IP-Adresse für Remotezugriff zuweisen.

Einstellen von Parametern

Um Parameter einzustellen, müssen Sie sich als Administrator anmelden. Auf der höchsten Ebene wird die Eingabeaufforderung `"Username" >` (Benutzername) angezeigt, der bei der Erstkonfiguration `"admin"` lautet. Geben Sie den Befehl "top" ein, um zur höchsten Menüebene zurückzukehren.

Hinweis: Wenn Sie sich mit einem anderen Benutzernamen angemeldet haben, wird dieser anstatt "admin" angezeigt.

Einstellen von Netzwerkparametern

Netzwerkparameter werden mithilfe des Befehls "interface" konfiguriert:

```
admin > Config > Network > interface ipauto none ip
192.168.151.12 mask 255.255.255.0 gw 192.168.151.1
mode auto
```

Wenn der Befehl akzeptiert wird, trennt das Gerät automatisch die Verbindung. Sie müssen die Verbindung zum Gerät unter Verwendung der neuen IP-Adresse und des Benutzernamens und des Kennworts, die Sie im Abschnitt zum Zurücksetzen des werkseitigen Standardkennworts erstellt haben, erneut herstellen.

Wichtig: Wenn Sie das Kennwort vergessen, muss LX über die Taste "Reset" (Zurücksetzen) auf der Rückseite von LX auf die Werkseinstellungen zurückgesetzt werden. Die Schritte zur Erstkonfiguration müssen in diesem Fall erneut durchgeführt werden.

LX verfügt nun über die Grundkonfiguration, und Sie können von einem Remotestandort aus (SSH oder GUI) sowie lokal mithilfe des lokalen seriellen Ports auf die Einheit zugreifen. Der Administrator muss Benutzer und Gruppen, Dienste, Sicherheit und serielle Ports, über die die seriellen Zielgeräte an LX angeschlossen sind, konfigurieren.

Eingabeaufforderungen der Befehlszeilenschnittstelle

Die Eingabeaufforderung der Befehlszeilenschnittstelle zeigt die aktuelle Befehlsebene an. Die Stammebene der Eingabeaufforderung ist der Anmeldename. Bei einer direkten Verbindung mit dem seriellen Port "Admin" mit einem Terminalemulationsprogramm ist "Admin Port" (Admin-Port) die Stammebene eines Befehls:

```
admin >
```

Bei SSH ist "admin" die Stammebene des Befehls:



```
admin > config > network >
```

0

Befehle der Befehlszeilenschnittstelle

- Geben Sie `admin > help` ein.

Befehl	Beschreibung
config	Wechselt zum Konfigurationsuntermenü.
diagnostics	Wechselt zum Diagnoseuntermenü.
help	Zeigt einen Überblick der Befehle an.
history	Anzeigen des Befehlszeilenverlaufs der aktuellen Sitzung.
listports	Listet die verfügbaren Ports auf.
logout	Abmelden von der aktuellen Sitzung der Befehlszeilenschnittstelle.
top	Rückkehr zum Stammmenü.
userlist	Listet aktive Benutzersitzungen auf.

- Geben Sie `admin > config > network` ein.

Befehl	Beschreibung
help	Zeigt einen Überblick der Befehle an.
history	Anzeigen des Befehlszeilenverlaufs der aktuellen Sitzung.
interface	Einstellen/Empfangen von Netzwerkparametern
ipv6_interface	Einstellen/Empfangen von IPv6-Netzwerkparametern
logout	Abmelden von der aktuellen Sitzung der Befehlszeilenschnittstelle.
name	Gerätenamenkonfiguration
quit	Kehrt zum vorherigen Menü zurück.
stop	Rückkehr zum Stammmenü.



Sicherheitsprobleme

Wichtige Elemente, die Sie bei der Sicherheit für Konsolenserver beachten sollten:

- Verschlüsselung des Datenverkehrs zwischen Bedienerkonsole und dem LX-Gerät
- Authentifizierung und Autorisierung von Benutzern
- Sicherheitsprofil

LX unterstützt diese drei Elemente. Sie müssen jedoch vor dem Gebrauch konfiguriert werden.

Verwalten der Befehle für die Konsolenserverkonfiguration von LX

Hinweis: Die Befehle der Kommandozeilenschnittstelle bleiben für SSH- und lokale Portzugriffssitzungen gleich.

Auf den Netzwerkbefehl kann über das Menü "Configuration" (Konfiguration) des LX zugegriffen werden.

Konfigurieren des Netzwerks

Die Netzwerkmenübefehle werden verwendet, um den LX-Netzwerkadapter zu konfigurieren.

Befehle	Beschreibung
interface	Konfiguriert die Netzwerkschnittstelle des LX-Geräts.
name	Netzwerknamenkonfiguration
ipv6	Einstellen/Empfangen von IPv6-Netzwerkparametern



Befehl "interface"

Der Befehl "interface" wird zur Konfiguration der Netzwerkschnittstelle des LX verwendet. Verwenden Sie folgende Syntax für den Befehl "interface":

```
interface [ipauto <none|dhcp>] [ip <ipaddress>]
[mask <subnetmask>] [gw <ipaddress>] [mode <mode>]

Einstellen/Empfangen von Ethernet-Parametern

ipauto <none|dhcp> IP auto configuration (none/dhcp)

ip <ipaddress> IP Address

mask <subnetmask> Subnet Mask

gw <ipaddress> Gateway IP Address

mode <mode> Set Ehternet Mode
(auto/10hdx/10fdx/100hdx/100fdx/1000fdx)
```

Beispiel für den Befehl "interface"

Der folgende Befehl aktiviert die Schnittstelle Nr. 1, legt die IP-Adresse, Maske und Gateway-Adressen sowie den Modus auf automatische Erkennung fest.

```
Admin > Config > Network > interface ipauto none ip
192.16.151.12 mask 255.255.255.0 gw 192.168.51.12
mode auto
```

Befehl "name"

Der Befehl "name" wird zur Konfiguration des Netzwerknamens verwendet. Verwenden Sie folgende Syntax für den Namen:

```
name [devicename <devicename>] [hostname <hostname>]
```

Gerätenamenkonfiguration

```
devicename <devicename>   Device Name

hostname   <hostname>     Preferred host name (DHCP
only)
```

Beispiel für den Befehl "name"

Folgender Befehl legt den Netzwerknamen fest:

```
Admin > Config > Network > name devicename My-KSX2
```

Befehl "IPv6"

Verwenden Sie den Befehl "IPv6", um die IPv6-Netzwerkparameter festzulegen und bestehende IPv6-Parameter abzurufen.



Kapitel 11 Lokale LX-Konsole

In diesem Kapitel

Überblick

Sie können am Serverschrank über den lokalen Port auf LX zugreifen und die Einheit verwalten. Dieser lokale Port bietet eine browserbasierte grafische Benutzeroberfläche, mit der Sie schnell und komfortabel zwischen den Servern wechseln können. Die lokale LX-Konsole stellt eine direkte analoge Verbindung mit den angeschlossenen Servern her. Die Leistung ist mit der Leistung bei einer direkten Verbindung mit der Tastatur, der Maus und den Videoports des Servers identisch. Die lokale LX-Konsole bietet dieselben Verwaltungsfunktionen wie die LX-Remotekonsole.

Gleichzeitige Benutzer

Die lokale LX-Konsole stellt einen unabhängigen Zugriffspfad zu den angeschlossenen KVM-Zielservern bereit. Die Verwendung der lokalen Konsole hindert andere Benutzer nicht daran, gleichzeitig eine Netzwerkverbindung herzustellen. Auch wenn Remotebenutzer mit LX verbunden sind, können Sie gleichzeitig über die lokale Konsole im Serverschrank auf die Server zugreifen.

Oberfläche der lokalen LX-Konsole: LX-Geräte

Am Serverschrank erfüllt LX über die lokale LX-Konsole standardmäßige KVM-Management- und Verwaltungsfunktionen. Die lokale LX-Konsole stellt eine direkte KVM-Verbindung (analog) mit den angeschlossenen Servern her. Die Leistung ist mit der Leistung bei einer direkten Verbindung mit der Tastatur, der Maus und den Videoports des Servers identisch.

Die grafischen Benutzeroberflächen der lokalen LX-Konsole und der LX-Remotekonsole verfügen über zahlreiche Gemeinsamkeiten. Auf die Unterschiede wird in diesem Hilfedokument hingewiesen.

Die LX-Option "Local Console Factory Reset" (Werksrücksetzung der lokalen Konsole) ist bei der lokalen LX-Konsole verfügbar, jedoch nicht bei der LX-Remotekonsole.

Sicherheit und Authentifizierung

Zur Verwendung der lokalen LX-Konsole müssen Sie zunächst mit einem gültigen Benutzernamen und Kennwort authentifiziert werden. LX verfügt über ein vollständig integriertes Authentifizierungs- und Sicherheitsschema, unabhängig davon, ob Sie über das Netzwerk oder den lokalen Port auf das Gerät zugreifen. In jedem Fall ermöglicht LX den Zugriff nur auf die Server, für die ein Benutzer über eine Zugriffsberechtigung verfügt. Weitere Informationen zum Festlegen des Serverzugriffs und der Sicherheitseinstellungen finden Sie unter ***Benutzerverwaltung*** (siehe "***User Management (Benutzerverwaltung)***" auf Seite 110).

Wenn Ihr LX für externe Authentifizierungsdienste (LDAP/LDAPS, RADIUS oder Active Directory) konfiguriert wurde, werden Authentifizierungsversuche in der lokalen Konsole auch durch den externen Authentifizierungsdienst authentifiziert.

Hinweis: Sie können für den lokalen Konsolenzugriff auch festlegen, dass keine Authentifizierung erfolgen soll. Diese Option wird jedoch nur für sichere Umgebungen empfohlen.

- **So verwenden Sie die lokale LX-Konsole:**

1. Schließen Sie an die lokalen Ports auf der Rückseite des LX-Geräts eine Tastatur, eine Maus und eine Videoanzeige an.
2. Starten Sie LX. Die Oberfläche der lokalen LX-Konsole wird angezeigt.



Unterstützte Videoauflösungen – Lokale Konsole

Stellen Sie sicher, dass die Videoauflösung und die Aktualisierungsfrequenz aller Zielserver von LX unterstützt werden und das Signal keinen Zeilensprung beinhaltet.

Die lokale LX-Konsole bietet folgende Auflösungen, um verschiedene Monitore zu unterstützen:

- 800x600
- 1024x768
- 1280x1024

Alle Auflösungen unterstützen eine Aktualisierungsfrequenz von 60 Hz und 75 Hz.

Die Videoauflösung und die Kabellänge sind wichtige Faktoren für die Maussynchronisierung. Siehe ***Verbindungsentfernung zum Zielserver und Videoauflösung*** (auf Seite 232).

Seite "Port Access" (Portzugriff) (Anzeige des lokalen Konsolenservers)

Nachdem Sie sich bei der lokalen LX-Konsole angemeldet haben, wird die Seite "Port Access" (Portzugriff) angezeigt. Diese Seite enthält alle LX-Ports, die angeschlossenen KVM-Zielserver sowie deren Status und Verfügbarkeit.

Wenn Sie eine Schichtkonfiguration verwenden, in der ein LX-Basisgerät für den Zugriff auf mehrere andere Schichtgeräte verwendet wird, werden die Schichtgeräte auf der Seite "Port Access" (Portzugriff) angezeigt, wenn Sie auf das Symbol "Expand Arrow" (Pfeil erweitern) ▶ links neben dem Schichtgerätenamen klicken. Weitere Informationen zu Schichten finden Sie unter ***Konfigurieren und Aktivieren von Schichten*** (auf Seite 142).

▶ So verwenden Sie die Seite "Port Access" (Port-Zugriff):

1. Melden Sie sich an der lokalen Konsole an.
2. Wählen Sie die Registerkarte "Port Access" (Portzugriff) aus. Die Seite "Port Access" (Port-Zugriff) wird angezeigt.

   Die KVM-Zielserver werden zuerst nach Portnummer sortiert. Sie können die Anzeige so ändern, dass nach einer beliebigen Spalte sortiert wird.

   - Port Number (Portnummer) – Die für das LX-Gerät verfügbaren Ports werden beginnend mit 1 durchnummeriert.

- Port Name (Portname) – Der Name des LX-Ports. Standardmäßig lautet dieser "Dominion-LX-Port#", Sie können den Namen jedoch durch einen aussagekräftigeren ersetzen. Wenn Sie auf einen Portnamenlink klicken, wird das Menü "Port Action" (Portaktion) geöffnet.

Hinweis: Verwenden Sie für den Port (CIM)-Namen keine Auslassungszeichen (Apostroph).

- "Type" (Typ) – Der Server- oder CIM-Typ.
- "Status" (Status) – Der Status für Standardserver lautet entweder "Up" (Ein) oder "Down" (Aus).
- "Availability" (Verfügbarkeit) – Die Verfügbarkeit des Servers.

3. Klicken Sie auf den Portnamen des Zielservers, auf den Sie zugreifen möchten. Das Menü "Port Action" (Portaktion) wird angezeigt. Informationen zu verfügbaren Menüoptionen finden Sie unter Menü "Port Action" (Portaktion).
4. Wählen Sie im Menü "Port Action" (Portaktion) den gewünschten Menübefehl aus.

So ändern Sie die Sortierreihenfolge der Anzeige und/oder zeigen mehr Ports auf einer Seite an:

1. Klicken Sie auf die Spaltenüberschrift, nach der sortiert werden soll. Die Liste der KVM-Zielserver wird nach dieser Spalte sortiert.
2. Geben Sie im Abschnitt "Rows per Page" (Zeilen pro Seite) die Anzahl der Ports ein, die auf der Seite angezeigt werden sollen, und klicken Sie dann auf "Set" (Festlegen).

Zugreifen auf einen Zielserver

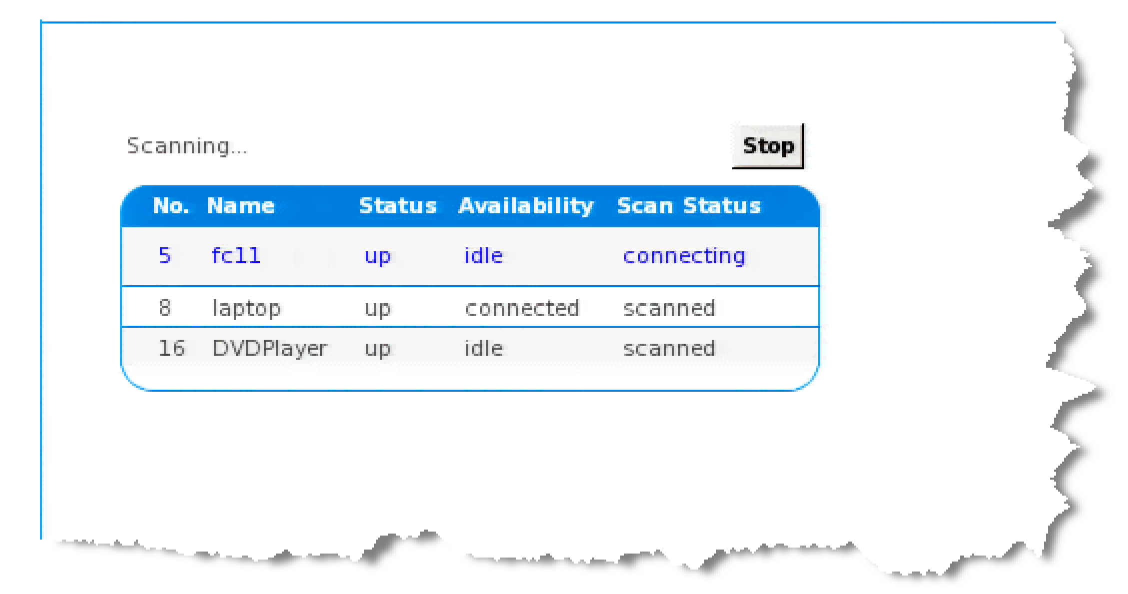
So greifen Sie auf einen Zielserver zu:

1. Klicken Sie auf den Portnamen des Zielgeräts, auf das Sie zugreifen möchten. Das Menü "Port Action" (Portaktion) wird angezeigt.
2. Wählen Sie im Menü "Port Action" (Portaktion) die Option "Connect" (Verbinden) aus. Die Videoanzeige wechselt zur Oberfläche des Zielservers.



Scannen von Ports – Lokale Konsole

Die Scanfunktion von LX wird von der lokalen Konsole unterstützt. Die während des Scanvorgangs gefundenen Ziele werden im Gegensatz zur Bildschirmpräsentation der Remotekonsole nacheinander auf der Seite "Scan" (Scannen) angezeigt. Jedes Ziel wird standardmäßig 10 Sekunden auf der Seite angezeigt, sodass Sie die Möglichkeit haben, eine Verbindung zum angezeigten Ziel herzustellen. Verwenden Sie die Tastenfolge "Local Port ConnectKey" (Verbindungstaste für lokalen Port), um eine Verbindung mit einem Ziel herzustellen, und die Tastenfolge "DisconnectKey" (Taste zum Trennen der Verbindung), um die Verbindung mit dem Ziel zu trennen.



▶ **So suchen Sie nach Zielen:**

1. Klicken Sie von der lokalen Konsole aus auf der Seite "Port Access" (Portzugriff) auf die Registerkarte "Set Scan" (Scanfunktion einstellen).
2. Wählen Sie die Ziele aus, die in die Suche einbezogen werden sollen, indem Sie das Kontrollkästchen links neben dem jeweiligen Ziel aktivieren. Durch Aktivieren des Kontrollkästchens oben in der Zielspalte können Sie auch alle Ziele auswählen.
3. Lassen Sie das Kontrollkästchen "Up Only" (Nur ein) aktiviert, wenn nur Ziele in die Suche einbezogen werden sollen, die eingeschaltet sind. Deaktivieren Sie dieses Kontrollkästchen, wenn Sie alle Ziele, egal ob ein- oder ausgeschaltet, in die Suche einbeziehen möchten.
4. Klicken Sie auf "Scan" (Scannen), um die Suche zu starten. Das Fenster "Port Scan" (Port-Scan) wird geöffnet. Jedes gefundene Ziel wird im Fenster angezeigt.



5. Stellen Sie mit der Tastenfolge "ConnectKey" (Verbindungstaste) eine Verbindung mit dem angezeigten Ziel her.
6. Klicken Sie auf "Stop Scan" (Scannen anhalten), um die Suche anzuhalten.

Verwenden von Scanoptionen

Die folgenden Optionen sind beim Scannen von Zielen verfügbar. Mit Ausnahme des Symbols "Expand/Collapse" (Erweitern/Reduzieren) können alle Optionen im Menü "Options" (Optionen) oben links in der Anzeige "Port Scan" (Port-Scan) ausgewählt werden. Beim Schließen des Fensters werden die Optionen auf die Standardeinstellungen zurückgesetzt.

Ausblenden oder Anzeigen von Miniaturansichten

- Mit dem Symbol "Expand/Collapse" (Erweitern/Reduzieren) oben links im Fenster können Sie Miniaturansichten ausblenden und anzeigen. Die erweiterte Ansicht ist die Standardeinstellung.

Pausieren der Bildschirmpräsentation von Miniaturansichten

- Unterbrechen Sie den Wechsel der Miniaturansichten zwischen einem Ziel und dem nächsten, indem Sie "Options" (Optionen) > "Pause" (Pausieren) auswählen. In der Standardeinstellung wird zwischen den Miniaturansichten gewechselt.

Pausieren der Bildschirmpräsentation von Miniaturansichten

- Setzen Sie den Wechsel zwischen den Miniaturansichten durch Auswählen von "Options" (Optionen) > "Resume" (Fortsetzen) fort.

Anpassen der Größe von Miniaturansichten in der Anzeige "Port Scan" (Port-Scan)

- Vergrößern Sie die Miniaturansichten, indem Sie "Options" (Optionen) > "Size" (Größe) > "360x240" auswählen.
- Zum Verkleinern der Miniaturansichten wählen Sie "Options" (Optionen) > "Size" (Größe) > "160x120" aus. Dies ist die Standardgröße für Miniaturansichten.

Ändern der Ausrichtung der Anzeige "Port Scan" (Port-Scan)

- Zum Anzeigen der Miniaturansichten am unteren Rand der Anzeige "Port Scan" (Port-Scan) wählen Sie "Options" (Optionen) > "Split Orientation" (Ausrichtung teilen) > "Horizontal".
- Zum Anzeigen der Miniaturansichten rechts in der Anzeige "Port Scan" (Port-Scan) wählen Sie "Options" (Optionen) > "Split Orientation" (Ausrichtung teilen) > "Vertical" (Vertikal). Dies ist die Standardansicht.



Zugriffstasten und Verbindungstasten

Da die Oberfläche der lokalen LX-Konsole vollständig durch die Oberfläche des Zielservers ersetzt wird, auf den Sie zugreifen, wird eine Zugriffstaste verwendet, um die Verbindung zu einem Ziel zu trennen und zur GUI des lokalen Ports zurückzukehren. Um eine Verbindung zu einem Ziel herzustellen oder zwischen Zielen zu wechseln wird eine Verbindungstaste verwendet.

Über die Zugriffstaste für den lokalen Port können Sie schnell die Benutzeroberfläche der lokalen LX-Konsole aufrufen, wenn gerade ein Zielserver angezeigt wird. Gemäß der Voreinstellung müssen Sie die Rollen-Taste zweimal kurz hintereinander drücken. Sie können jedoch [auf der Seite "Local Port Settings" (Lokale Porteinstellungen)] eine andere Tastenkombination als Zugriffstaste festlegen. Weitere Informationen finden Sie unter Lokale Porteinstellungen der lokalen LX-Konsole konfigurieren.

Beispiele für Verbindungstasten

Standardserver	
Funktion der Verbindungstaste	**Beispiel für Tastenfolge**
Auf einen Port über die GUI des lokalen Ports zugreifen	Zugriff auf Port 5 über die GUI des lokalen Ports: • Linke Alt-Taste drücken > Taste "5" drücken und wieder loslassen > Linke Alt-Taste wieder loslassen
Zwischen Ports wechseln	Von Port 5 auf Port 11 wechseln: • Linke Alt-Taste drücken > Taste "1" drücken und wieder loslassen > Taste "1" erneut drücken und wieder loslassen > Linke Alt-Taste wieder loslassen
Verbindung zu einem Zielgerät trennen und zur GUI des lokalen Ports zurückkehren	Verbindung zum Zielport 11 trennen und zur GUI des lokalen Ports zurückkehren (zu der Seite, von der aus Sie eine Verbindung zum Zielgerät hergestellt haben): • "Double Click Scroll Lock" (Rollen-Taste zweimal drücken)

Spezielle Tastenkombinationen für Sun

Die folgenden Tastenkombinationen für spezielle Tasten von Sun™ Microsystems-Servern sind für den lokalen Port verfügbar. Diese speziellen Tasten sind im Menü "Keyboard" (Tastatur) verfügbar, wenn Sie eine Verbindung zu einem Sun-Zielserver herstellen.

Sun-Taste	Tastenkombination für lokalen Port
Again	Strg+Alt+F2
Props	Strg+Alt+F3
Undo	Strg+Alt+F4
Stop A	Untbr a
Front	Strg+Alt+F5
Copy	Strg+Alt+F6
Open	Strg+Alt+F7
Find	Strg+Alt+F9
Cut	Strg+Alt+F10
Paste	Strg+Alt+F8
Mute (Stummschaltung)	Strg+Alt+F12
Compose	Strg+Alt+Nummernfeld *
Vol +	Strg+Alt+Nummernfeld +
Vol -	Strg+Alt+Nummernfeld -
Stop	Keine Tastenkombination
Stromversorgung	Keine Tastenkombination

Zurückkehren zur Oberfläche der lokalen LX-Konsole

Wichtig: Um über die Standardzugriffstaste auf die lokale LX-Konsole zuzugreifen, müssen Sie die Rollen-Taste zweimal kurz hintereinander drücken. Diese Tastenkombination können Sie auf der Seite "Local Port Settings" (Lokale Porteinstellungen) ändern. Siehe Konfigurieren der lokalen LX-Porteinstellungen von der lokalen Konsole aus.



So kehren Sie vom Zielserver zur lokalen LX-Konsole zurück:

- Drücken Sie die Zugriffstaste zweimal schnell hintereinander (die Standardzugriffstaste ist die Rollen-Taste). Die Videoanzeige wechselt von der Oberfläche des Zielservers zur Oberfläche der lokalen LX-Konsole.

Verwaltung über den lokalen Port

LX kann entweder über die lokale LX-Konsole oder die LX-Remotekonsole verwaltet werden. Beachten Sie, dass Sie über die lokale LX-Konsole auch Zugriff haben auf:

- Werksrücksetzung
- Lokale Porteinstellungen(auch für die Remotekonsole verfügbar)

Hinweis: Auf diese Funktionen können nur Benutzer mit Administratorrechten zugreifen.

Lokale Porteinstellungen der lokalen LX-Konsole konfigurieren

Auf der Seite "Local Port Settings" (Lokale Porteinstellungen) können Sie viele Einstellungen für die lokale LX-Konsole anpassen. Dazu zählen die Tastatur, die Zugriffstasten, die Verzögerung beim Videowechsel, der Stromsparmodus, die Auflösungseinstellungen für die lokale Benutzeroberfläche sowie die lokale Benutzerauthentifizierung.

Hinweis: Auf diese Funktionen können nur Benutzer mit Administratorrechten zugreifen.

So konfigurieren Sie die lokalen Porteinstellungen:

Hinweis: Einige Einstellungsänderungen, die auf der Seite "Local Port Settings" (Lokale Porteinstellungen) vorgenommen werden, führen zum Neustart des verwendeten Browsers. Führt eine Einstellungsänderung zum Neustart des Browser, so ist dies in den hier beschriebenen Schritten vermerkt.

1. Wählen Sie "Device Settings" > "Local Port Settings" (Geräteeinstellungen > Lokale Porteinstellungen) aus. Die Seite "Local Port Settings" (Lokale Porteinstellungen) wird angezeigt.
2. Aktivieren Sie das Kontrollkästchen neben "Enable Standard Local Port" (Lokalen Standardport aktivieren). Deaktivieren Sie das Kontrollkästchen, um den Port zu deaktivieren. Der lokale Standardport ist standardmäßig aktiviert, kann jedoch bei Bedarf aktiviert werden. Wenn Sie die Schichtfunktion verwenden, ist diese Funktion deaktiviert, da beide Funktionen nicht gleichzeitig verwendet werden können.

3. Wenn Sie die Schichtfunktion verwenden, wählen Sie das Kontrollkästchen "Enable Local Port Device Tiering" (Geräteschicht für lokalen Port aktivieren) aus und geben den geheimen Schlüssel für die Schicht in das Feld "Tier Secret" (Geheimer Schlüssel der Schicht) ein. Um die Schichten zu konfigurieren, müssen Sie auch das Basisgerät auf der Seite "Device Services" (Gerätedienste) konfigurieren. Weitere Informationen zu Schichten finden Sie unter ***Konfigurieren und Aktivieren von Schichten*** (auf Seite 142).
4. Konfigurieren Sie ggf. die Einstellungen "Local Port Scan Mode" (Scanmodus für den lokalen Port). Diese Einstellungen gelten für das Feature "Scan Settings" (Scaneinstellungen), auf das Sie über die Seite "Port" zugreifen. Siehe ***Scannen von Ports*** (auf Seite 51).
   - Geben Sie im Feld "Display Interval (10-255 sec):" (Anzeigeintervall (10-255 Sek.)) die Anzahl Sekunden ein, die das Ziel im Fokus in der Mitte des Fensters "Port Scan" (Port-Scan) angezeigt werden soll.
   - Geben Sie im Feld "Interval Between Ports (10 - 255 sec):" (Intervall zwischen Ports (10 – 255 Sek.)) das Intervall ein, in dem das Gerät zwischen Ports pausieren soll.
5. Wählen Sie aus den Optionen in der Dropdown-Liste den geeigneten Tastaturtyp aus. Der Browser wird neu gestartet, nachdem diese Änderung durchgeführt wurde.
   - US
   - US/International (USA/International)
   - United Kingdom (Großbritannien)
   - French (France) (Französisch)
   - German (Germany) (Deutsch)
   - JIS (Japanese Industry Standard) (Japanisch [Japanischer Branchenstandard])
   - Simplified Chinese (Vereinfachtes Chinesisch)
   - Traditional Chinese (Traditionelles Chinesisch)
   - Dubeolsik Hangul (Korean) (Koreanisch)
   - German (Deutsch, Schweiz)
   - Portugiesisch (Portugal)
   - Norwegian (Norway) (Norwegisch)
   - Swedish (Sweden) (Schwedisch)
   - Danish (Denmark) (Dänisch)
   - Belgian (Belgium) (Belgisch)



Hinweis: Sie können die Tastatur für Chinesisch, Japanisch und Koreanisch nur für die Anzeige verwenden. Für Funktionen der lokalen LX-Konsole werden Eingaben in diesen Sprachen derzeit nicht unterstützt.

Hinweis: Bei Verwendung einer türkischen Tastatur müssen Sie die Verbindung mit einem Zielserver über den Active KVM Client (AKC) herstellen. Von anderen Raritan-Clients wird es nicht unterstützt.

6. Wählen Sie die Zugriffstaste für den lokalen Port. Über die Zugriffstaste für den lokalen Port können Sie zur Benutzeroberfläche der lokalen LX-Konsole zurückkehren, wenn gerade eine Zielserveroberfläche angezeigt wird. Die Standardoption lautet "Double Click Scroll Lock" (Rollen-Taste zweimal drücken). Sie können jedoch eine andere Tastenkombination aus der Dropdownliste auswählen.

Zugriffstaste	Zu drückende Tastenkombination
Rollen-Taste zweimal drücken	Drücken Sie die Rollen-Taste zweimal kurz hintereinander.
Num-Feststelltaste zweimal drücken	Drücken Sie die Num-Feststelltaste zweimal kurz hintereinander.
Feststelltaste zweimal drücken	Drücken Sie die Feststelltaste zweimal kurz hintereinander.
Linke Alt-Taste zweimal drücken	Drücken Sie die linke Alt-Taste zweimal kurz hintereinander.
Linke Umschalttaste zweimal drücken	Drücken Sie die linke Umschalttaste zweimal kurz hintereinander.
Linke Strg-Taste zweimal drücken	Drücken Sie die linke Strg-Taste zweimal kurz hintereinander.

7. Wählen Sie die Verbindungstaste für den lokalen Port aus. Verwenden Sie eine Verbindungstastenfolge, um eine Verbindung mit einem Zielgerät herzustellen und zu einem anderen Zielgerät zu wechseln. Sie können anschließend die Zugriffstaste verwenden, um die Verbindung zum Zielgerät zu trennen und zur GUI des lokalen Ports zurückzukehren. Wenn die Verbindungstaste für den lokalen Port erstellt wurde, erscheint diese im Navigationsfenster der GUI, sodass Sie sie als Referenz verwenden können. Beispiele für Verbindungstastenfolgen finden Sie unter Beispiele für Verbindungstasten.
8. Klicken Sie auf OK.



Werksrücksetzung der lokalen LX-Konsole

Hinweis: Dieses Feature ist nur für die lokale LX-Konsole verfügbar.

LX bietet über die Benutzeroberfläche der lokalen Konsole verschiedene Rücksetzungsmodi.

Hinweis: Bevor Sie die Einheit auf die Werkseinstellungen zurücksetzen, sollten Sie das Prüfprotokoll speichern. Das Prüfprotokoll wird bei der Zurücksetzung auf die Werkseinstellungen gelöscht, und dieses Ereignis wird nicht protokolliert. Weitere Informationen zum Speichern des Prüfprotokolls finden Sie unter ***Prüfprotokoll*** *(siehe "****Audit Log (Prüfprotokoll)****" auf Seite 175).*

So führen Sie eine Werksrückstellung durch:

1. Wählen Sie "Maintenance" > "Factory Reset" (Wartung > Werksrücksetzung) aus. Die Seite "Factory Reset" (Werksrücksetzung) wird angezeigt.
2. Wählen Sie die entsprechende Rücksetzungsoption aus:
   - "Full Factory Reset" (Vollständige Werksrücksetzung) – Damit entfernen Sie die gesamte Konfiguration und setzen das Gerät komplett auf die werkseitigen Standardeinstellungen zurück. Beachten Sie, dass Verwaltungsverbindungen mit CommandCenter dadurch unterbrochen werden. Da diese Rückstellung so umfassend ist, werden Sie dazu aufgefordert, den Vorgang zu bestätigen.
   - "Network Parameter Reset" (Netzwerkparameterrücksetzung) – Damit setzen Sie die Netzwerkparameter des Geräts auf die Standardwerte zurück [Klicken Sie auf "Device Settings" > "Network Settings" (Geräteeinstellungen > Netzwerkeinstellungen), um auf diese Informationen zuzugreifen]:



- Automatische IP-Konfiguration
- IP-Adresse
- Subnet Mask (Subnetzmaske)
- Gateway-IP-Adresse
- IP-Adresse des primären DNS-Servers
- IP-Adresse des sekundären DNS-Servers
- Discovery Port (Erkennungsport)
- Bandwidth Limit (Maximale Bandbreite)
- LAN Interface Speed & Duplex (LAN-Schnittstellengeschwindigkeit & Duplex)

3. Klicken Sie auf "Reset" (Zurücksetzen), um fortzufahren. Da hierbei alle Netzwerkeinstellungen verloren gehen, werden Sie aufgefordert, die Werksrücksetzung zu bestätigen.
4. Klicken Sie zum Fortfahren auf "OK". Nach Abschluss des Vorgangs wird das LX-Gerät automatisch neu gestartet.

Zurücksetzen des LX mithilfe der Taste "Reset" (Zurücksetzen)

Auf der Rückseite des Geräts befindet sich die Taste "Reset" (Zurücksetzen). Sie ist etwas zurückgesetzt, damit sie nicht unbeabsichtigt gedrückt wird (Sie benötigen einen spitzen Gegenstand, um die Taste zu betätigen).

Welche Maßnahmen ergriffen werden, wenn die Taste "Reset" (Zurücksetzen) gedrückt wird, legen Sie über die grafische Benutzeroberfläche fest. Siehe ***Encryption & Share (Verschlüsselung und Freigabe)*** (auf Seite 168).

Hinweis: Bevor Sie die Einheit auf die Werkseinstellungen zurücksetzen, sollten Sie das Prüfprotokoll speichern. Das Prüfprotokoll wird bei der Zurücksetzung auf die Werkseinstellungen gelöscht, und dieses Ereignis wird nicht protokolliert. Weitere Informationen zum Speichern des Prüfprotokolls finden Sie unter **Prüfprotokoll** *(siehe "***Audit Log (Prüfprotokoll)***" auf Seite 175).*

So setzen Sie das Gerät zurück:

1. Schalten Sie die LX-Einheit aus.
2. Verwenden Sie einen spitzen Gegenstand, und halten Sie die Taste zum Zurücksetzen damit gedrückt.
3. Halten Sie die Taste zum Zurücksetzen gedrückt und schalten Sie gleichzeitig das LX-Gerät wieder ein.

4. Halten Sie die Taste "Reset" (Zurücksetzen) weitere zehn Sekunden gedrückt. Wenn das Gerät vollständig zurückgesetzt wurde, ertönen zwei kurze Tonsignale.





Anhang A Technische Daten

In diesem Kapitel

LX-Spezifikationen

Dominion LX-Modell	**Beschreibung**	**Produktabmessungen (B x T x H), Liefergewicht und Stromversorgung**	**Umgebung**
DLX-108	[illegible]	11,45" x 10,63 " x 1,73"; 291 mm x 270 mm x 44 mm 8,82 lbs; 4,0 kg Einzelstromversorgung 100-240 V AC, 50-60 Hz, 0,5 A, 30 Watt, 25,794 kcal/h	Betriebstemperatur: 0°C bis 40°C (32°F bis 104°F) Luftfeuchtigkeit: 20 % bis 85 % relative Luftfeuchtigkeit



	erweiterbarer KVM-über-IP-Switch mit 8 Ports, 1 Pen		



	otebenutzer, 1 lokaler Benutzer, virtuelle Medien, B		



	inzelstromversorgung und ein LAN-Anschluss		
DLX-116	Ökonomis		



	cher, erweiterbarer KVM-über-IP-Switch mit 16 Ports,		



	1 Remotebenutzer, 1 lokaler Benutzer, virtuelle Me		



	dien, Einzelstromversorgung und ein LAN-Anschluss		
DLX-216	Ök [illegible]		



	onomischer, erweiterbarer KVM-über-IP-Switch mit 16		



	Ports, 2 Remotebenutzer, 1 lokaler Benutzer, virtue		



	lle Medien, Einzelstromversorgung und ein LAN-Ansch		



	l u s s
Hardware-unterstützt	
Formfaktor	1U-Einschub (Halterungen im Lieferumfang enthalten)
Lokaler Zugriffsport	Video: HD15 (weiblich) VGA; Tastatur/Maus: USB (weiblich); 3 USB-Anschlüsse auf der Rückseite
Beispiele für Videoauflösungen	PC-Textmodus: 640x350, 640x480, 720x400 PC-Grafikmodus: 640x480, 800x600, 1024x768, 1152x864, 1280x1024, 1440x900, 1680x1050,1600x1200, 1920x1080 Sun-Videomodus: 1024x768, 1152x864, 1152x900, 1280x1024
Remoteverbindung	
Ports	8(DLX-108) oder 16 (DLX-116, DLX-216)
Benutzer	Lokaler Benutzer, 1 oder 2 Remotebenutzer (modellabhängig)
Network (Netzwerk)	10/100/1000-Gigabit-Ethernetzugriff, Dual-Stack-Architektur: IPv4 und IPv6
Protokolle	TCP/IP, HTTP, HTTPS, UDP, RADIUS, SNMP, DHCP, PAP, CHAP
Computer Interface Modules (CIMs) und Cat5-Kabel	
Dominion CIMs	Verfügbar für USB, Dual USB, Universal Virtual Media/Absolute Mouse Synchronization, PS2, Sun, Serielle Geräte Abmessungen (B x T x H) = 1,7" x 3,5" x 0,8", 43 mm x 90 mm x 19 mm (Dual USB) und 1,3" x 3,0" x 0,6", 33 mm x 76 mm x 15 mm (andere DCIMs)
Cat5-Kabel für MCUTP	KVM-UTP-Kabel für PS/2, USB, Sun – Länge von 0,6 m bis 6 m Technische Daten: RJ45 <-> HDB-15M, Mini-DIN 6 x 2 (PS/2), USB Typ A (USB/Sun)
Service und Support	
Garantie*	Standardmäßig 2 Jahre mit erweitertem Austausch

LED-Anzeigen

LED-Anzeige an der Vorderseite

- Hochfahren – Blaue und rote LEDs = eingeschaltet
- In Betrieb – Nur blaue LED
- Firmwareaktualisierung – Blaue LED blinkt

LED-Anzeige an der Rückseite

- "10 Mbps/Half" (10 Mbit/s/Halb) – Beide LEDs blinken
- "10 Mbps/Full" (10 Mbit/s/Voll) – Beide LEDs blinken
- "100 Mbps/Half" (10 Mbit/s/Halb) – Gelbe LED blinkt
- "1 Gbps/Full" (1 GB/s/Voll) – Grüne LED blinkt

Unterstützte Betriebssysteme (Clients)

Die folgenden Betriebssysteme werden auf dem Virtual KVM Client und dem Multi-Platform-Client (MPC) unterstützt:

Client-Betriebssystem	Unterstützung virtueller Medien (VM) auf dem Client?
Windows 7®	Yes (Ja)
Windows XP®	Yes (Ja)
Windows 2008®	Yes (Ja)
Windows Vista®	Yes (Ja)
Windows 2000® SP4-Server	Yes (Ja)
Windows 2003® Server	Yes (Ja)
Windows 2008® Server	Yes (Ja)
Red Hat® Desktop 5.0	Yes (Ja)
Red Hat Desktop 4.0	Yes (Ja)
Open SUSE 10, 11	Yes (Ja)
Fedora® 13 und 14	Yes (Ja)
Mac® OS	Yes (Ja)
Solaris™	Nein



Client-Betriebssystem	Unterstützung virtueller Medien (VM) auf dem Client?
Linux®	Yes (Ja)

Das JRE™-Plug-in ist für Windows® 32-Bit- und 64-Bit-Betriebssysteme verfügbar. MPC und VKC können nur über einen 32-Bit-Browser und die 64-Bit-Browser IE7 oder IE8 gestartet werden.

Im Folgenden werden die Anforderungen von Java™ unter den Windows-Betriebssystemen (32 und 64 Bit) aufgelistet:

Modus	Betriebssystem	Browser
Windows x64 32-Bit-Modus	Windows XP®	• Internet Explorer® 6.0 SP1+ oder 7.0, IE 8 • Firefox® 1.06 - 3
	Windows Server 2003®	• Internet Explorer 6.0 SP1++, IE 7, IE 8 • Firefox 1.06 – 3
	Windows Vista®	• Internet Explorer 7.0 oder 8.0
	Windows 7®	• Internet Explorer 9,0 • Firefox 1.06 – 3
Windows x64 64-Bit-Modus	Windows XP	64-Bit-Betriebssystem, 32-Bit-Browser: • Internet Explorer 6.0 SP1+, 7.0 oder 8.0 • Firefox 1.06 – 3 64-Bit-Modus, 64-Bit-Browser: • Internet Explorer 7.0 oder 8.0
	Windows XP Professional®	
	Windows XP Tablet®	
	Windows Vista	
	Windows Server 2003	
	Windows Server 2008	
	Windows 7	

Unterstützte Browser

LX unterstützt die folgenden Browser:

- Internet Explorer® 6 bis 9
- Firefox® 1.5, 2.0, 3.0 (bis Build 3.6.17) und 4.0
- Safari® 3 oder höher



Unterstützte CIMs und Betriebssysteme

Zusätzlich zu den D2CIMs werden die meisten Dominion CIMs unterstützt. Die folgende Tabelle enthält die unterstützten Betriebssysteme, CIMs, virtuellen Medien und Mausmodi auf Zielservern.

Hinweis: D2CIM-VUSB wird auf Sun™ (Solaris™)-Zielen nicht unterstützt.

Unterstützte LX-D2CIMs	Zielserver und Remote-Gestell-PDUs (wenn zutreffend)	Virtuelle Medien	Mausmodus "Absolut"	Mausmodu s "Intelligent"	Ma s "S
D2CIM-VUSB	• Windows XP • Windows 2000 • Windows 2000 Server • Windows 2003 Server • Windows Vista • Windows 7 • Windows 2008 • Open SUSE 10, 11 • Fedora Core 3 und höher • Mac OS	✓	✓	✓	✓
	• Red Hat Enterprise Linux 4 ES • Red Hat Enterprise Linux 5	✓		✓	✓
D2CIM-DVUSB	• Windows XP • Windows 2000 • Windows 2000 Server • Windows 2003 Server • Windows Vista • Windows 7 • Windows 2008 • Open SUSE 10, 11 • Fedora 8-11	✓	✓	✓	✓



Unterstützte LX-D2CIMs	Zielserver und Remote-Gestell-PDUs (wenn zutreffend)	Virtuelle Medien	Mausmodus "Absolut"	Mausmodus "Intelligent"	Ma s "S
	• Mac OS				
	• Red Hat Enterprise Linux 4 ES • Red Hat Enterprise Linux 5	✓		✓	✓

Unterstützte Videoauflösungen

Stellen Sie sicher, dass die Videoauflösung und die Aktualisierungsfrequenz aller Zielserver von LX unterstützt werden und das Signal keinen Zeilensprung beinhaltet.

Die Videoauflösung und die Kabellänge sind wichtige Faktoren für die Maussynchronisierung. Siehe ***Verbindungsentfernung zum Zielserver und Videoauflösung*** (auf Seite 232).

Die folgenden Auflösungen werden von LX unterstützt:

Auflösungen	
640 x 350 bei 70Hz	1024 x 768 bei 85Hz
640 x 350 bei 85Hz	1024 x 768 bei 75Hz
640 x 400 bei 56Hz	1024 x 768 bei 90Hz
640 x 400 bei 84Hz	1024 x 768 bei 100Hz
640 x 400 bei 85Hz	1152 x 864 bei 60Hz
640 x 480 bei 60Hz	1152 x 864 bei 70Hz
640 x 480 bei 66,6Hz	1152 x 864 bei 75Hz
640 x 480 bei 72Hz	1152 x 864 bei 85Hz
640 x 480 bei 75Hz	1.152 x 870 bei 75,1Hz
640 x 480 bei 85Hz	1.152 x 900 bei 66Hz
720 x 400 bei 70Hz	1.152 x 900 bei 76Hz
720 x 400 bei 84Hz	1.280 x 720 bei 60Hz



Auflösungen	
720 x 400 bei 85Hz	1.280 x 960 bei 60Hz
800 x 600 bei 56Hz	1.280 x 960 bei 85Hz
800 x 600 bei 60Hz	1280 x 1024 bei 60Hz
800 x 600 bei 70Hz	1280 x 1024 bei 75Hz
800 x 600 bei 72Hz	1280 x 1024 bei 85Hz
800 x 600 bei 75Hz	1.360 x 768 bei 60Hz
800 x 600 bei 85Hz	1.366 x 768 bei 60Hz
800 x 600 bei 90Hz	1.368 x 768 bei 60Hz
800 x 600 bei 100Hz	1.400 x 1050 bei 60Hz
832 x 624 bei 75,1Hz	1.440 x 900 bei 60Hz
1024 x 768 bei 60Hz	1600 x 1200 bei 60Hz
1024 x 768 bei 70Hz	1.680 x 1.050 bei 60Hz
1024 x 768 bei 72Hz	1920 x 1080 bei 60Hz

Verbindungsentfernung zum Zielserver und Videoauflösung

Die maximal unterstützte Entfernung hängt von mehreren Faktoren ab. Dazu gehören der Typ/die Qualität des Kabels der Kategorie 5, der Servertyp und -hersteller, der Videotreiber und Monitor, die Umgebungsbedingungen und die Erwartungen des Benutzers. Bei den Videoauflösungen von 1600x1200 und 1920x1080 beträgt die Aktualisierungsfrequenz 60 und die maximale Verbindungsentfernung 15 m.

Hinweis: Aufgrund der Vielzahl an Serverherstellern und -typen, Betriebssystemversionen, Videotreibern usw. sowie der subjektiven Auffassung von Videoqualität kann Raritan nicht für die Leistung bei allen Entfernungen in allen Umgebungen garantieren.

Von LX unterstützte Videoauflösungen finden Sie unter ***Unterstützte Videoauflösungen*** (auf Seite 14).



Zertifizierte Modems

- USRobotics® 56K 5686E
- ZOOM® v90
- ZOOM v92
- USRobotics Sportster® 56K
- USRobotics Courier™ 56K

Remoteverbindung

Remoteverbindung	Details
Network (Netzwerk)	10BASE-T-, 100BASE-T- und 1000BASE-T (Gigabit)-Ethernet
Protokolle	TCP/IP, UDP, SNTP, HTTP, HTTPS, RADIUS, LDAP/LDAPS

Unterstützte Tastatursprachen

LX bietet Tastaturunterstützung für die in der folgenden Tabelle aufgeführten Sprachen.

Hinweis: Sie können die Tastatur für Chinesisch, Japanisch und Koreanisch nur für die Anzeige verwenden. Für Funktionen der lokalen LX-Konsole werden Eingaben in diesen Sprachen derzeit nicht unterstützt. Weitere Informationen zu nicht US-amerikanischen Tastaturen finden Sie unter **Wichtige Hinweise** *(auf Seite 249).*

Hinweis: Raritan empfiehlt Ihnen für Änderungen der Spracheinstellungen die Verwendung von "system-config-keyboard", wenn Sie in einer Linux-Umgebung arbeiten.

Sprache	Regionen	Tastaturlayout
US English (Englisch USA)	Vereinigte Staaten von Amerika und die meisten englischsprachigen Länder: z. B. Kanada, Australien und Neuseeland.	US-amerikanisches Tastaturlayout
US English International (Englisch USA/International)	Vereinigte Staaten von Amerika und die meisten englischsprachigen Länder: z. B. die Niederlande.	US-amerikanisches Tastaturlayout



Sprache	Regionen	Tastaturlayout
UK English (Englisch Großbritannien)	United Kingdom (Großbritannien)	Englisches Tastaturlayout (Großbritannien)
Chinese Traditional (Traditionelles Chinesisch)	Hongkong, Republik China (Taiwan)	Chinese Traditional (Traditionelles Chinesisch)
Chinese Simplified (Vereinfachtes Chinesisch)	Festland der Volksrepublik China	Chinese Simplified (Vereinfachtes Chinesisch)
Korean (Koreanisch)	Südkorea	Dubeolsik Hangul
Japanese (Japanisch)	Japan	JIS-Tastatur (Japanischer Branchenstandard)
French (Französisch)	Frankreich	Französisches (AZERTY-)Tastaturlayout
German (Deutsch)	Deutschland und Österreich	Deutsche Tastatur (QWERTZ-Layout)
French (Französisch)	Belgien	Belgian (Belgisch)
Norwegian (Norwegisch)	Norwegen	Norwegian (Norwegisch)
Danish (Dänisch)	Dänemark	Danish (Dänisch)
Swedish (Schwedisch)	Schweden	Swedish (Schwedisch)
Hungarian (Ungarisch)	Ungarn	Hungarian (Ungarisch)
Slovenian (Slowenisch)	Slowenien	Slovenian (Slowenisch)
Italian (Italienisch)	Italien	Italian (Italienisch)
Spanish (Spanisch)	Spanien und die meisten spanischsprachigen Länder	Spanish (Spanisch)
Portuguese (Portugiesisc	Portugal	Portuguese



Sprache	Regionen	Tastaturlayout
h)		(Portugiesisch)

Verwendete TCP- und UDP-Ports

Port	Beschreibung
HTTP, Port 80	Dieser Port kann bei Bedarf konfiguriert werden. Siehe ***HTTP- und HTTPS-Porteinstellungen*** (auf Seite 140). Alle von LX über HTTP (Port 80) empfangenen Anforderungen werden standardmäßig zur Gewährleistung der Sicherheit automatisch an HTTPS weitergeleitet. LX beantwortet Anforderungen aus Gründen der Benutzerfreundlichkeit über Port 80. Auf diese Weise müssen Benutzer für den Zugriff auf LX im URL-Feld keine Eingaben vornehmen. Die Sicherheit ist jedoch vollständig gewährleistet.
HTTPS, Port 443	Dieser Port kann bei Bedarf konfiguriert werden. Siehe ***HTTP- und HTTPS-Porteinstellungen*** (auf Seite 140). Dieser Port wird standardmäßig für verschiedene Zwecke verwendet, z. B. für den Webserver des HTML-Clients, das Herunterladen von Clientsoftware (MPC/VKC) auf den Clienthost oder die Übertragung von KVM- oder virtuellen Mediendatenströmen zum Client.
LX-Protokoll (Raritan KVM-über-IP), konfigurierbarer Port 5000	Dieser Port wird zur Erkennung anderer Dominion-Geräte und zur Kommunikation zwischen Raritan-Geräten und -Systemen verwendet. Standardmäßig ist der Port 5000 eingestellt. Sie können jedoch jeden anderen TCP-Port konfigurieren, der nicht verwendet wird. Informationen zum Konfigurieren dieser Einstellung finden Sie unter ***Netzwerkeinstellungen*** (siehe "***Network Settings (Netzwerkeinstellungen)***" auf Seite 134).
SNTP (Zeitserver) über den konfigurierbaren UDP-Port 123	LX bietet optional die Möglichkeit, die interne Uhr mit einem zentralen Zeitserver zu synchronisieren. Diese Funktion erfordert die Verwendung des UDP-Ports 123 (Standardport für SNTP), sie kann jedoch auch zur Verwendung eines anderen Ports Ihrer Wahl konfiguriert werden. **///Optional**
LDAP/LDAPS über den konfigurierbaren Port 389 oder 936	Wenn LX zur Remoteauthentifizierung von Benutzeranmeldungen über das LDAP-/LDAPS-Protokoll konfiguriert ist, wird Port 389 oder 636 verwendet. Das System kann jedoch auch zur Verwendung eines anderen Ports Ihrer Wahl konfiguriert werden. **Optional**
RADIUS über den konfigurierbaren Port 1812	Wenn LX zur Remoteauthentifizierung von Benutzeranmeldungen über das RADIUS-Protokoll konfiguriert ist, wird Port 1812 verwendet. Das System kann jedoch auch zur Verwendung eines anderen Ports Ihrer Wahl konfiguriert werden. **Optional**
RADIUS-Kontoführung über den konfigurierbaren Port 1813	Wenn LX zur Remoteauthentifizierung von Benutzeranmeldungen über das RADIUS-Protokoll konfiguriert ist und auch die RADIUS-Kontoführung zur Ereignisprotokollierung verwendet, wird Port 1813 oder ein zusätzlicher Port Ihrer Wahl zur Übertragung von Protokollbenachrichtigungen verwendet.
SYSLOG über den	Wenn LX zum Senden von Meldungen an einen Syslog-Server



konfigurierbaren UDP-Port 514	konfiguriert ist, werden die angegebenen Ports für die Kommunikation verwendet (verwendet UDP-Port 514).
SNMP-Standard-UDP-Ports	Port 161 wird für eingehende/ausgehende SNMP-Lese- und -Schreibvorgänge, Port 162 für ausgehenden Datenverkehr für SNMP-Traps verwendet. **///Optional**
TCP-Port 21	Port 21 wird für die Kommandozeilenschnittstelle des LX verwendet (wenn Sie mit dem technischen Kundendienst von Raritan zusammenarbeiten).

Im Prüfprotokoll und im Syslog erfasste Ereignisse

In der folgenden Liste werden die Ereignisse aufgeführt, die im Prüfprotokoll und Syslog von LX erfasst werden:

- "System Startup" (Systemstart)
- "System Shutdown" (Herunterfahren des Systems)
- "Network Parameter Changed" (Netzwerkparameter geändert)
- "Port Status Changed" (Portstatus geändert)
- "Network Failure" (Netzwerkfehler)
- "Communication Error" (Kommunikationsfehler)
- "Factory Reset" (Werksrückstellung)
- "Device Update Started" (Aktualisierung des Geräts gestartet)
- "Device Update Completed" (Aktualisierung des Geräts abgeschlossen)
- "Device Update Failed" (Aktualisierung des Geräts fehlgeschlagen)
- "Firmware Update Failed" (Firmwareaktualisierung fehlgeschlagen)
- "Firmware File Discarded" (Firmwaredatei verworfen)
- "Firmware Validation Failed" (Firmware-Validierung fehlgeschlagen)
- "Configuration Backed Up" (Konfiguration gesichert)
- "Configuration Restored" (Konfiguration wiederhergestellt)
- "Port Connection Denied" (Verbindung mit Port verweigert)
- "Active USB Profile" (aktives USB-Profil)
- "Certficiate Update" (Zertifikatsaktualisierung)
- "Date/Time Settings Changed" (Datum-/Uhrzeiteinstellungen geändert)
- "Password Settings Changed" (Kennworteinstellungen geändert)
- "Login Failed" (Anmeldung fehlgeschlagen)
- "Password Changed" (Kennwort geändert)
- "User Blocked" (Benutzer gesperrt)
- "Port Connected" (Port verbunden)
- "Port Disconnected" (Port getrennt)
- "Access Login" (Zugriffsanmeldung)
- "Access Logout" (Zugriffsabmeldung)
- "Connection Lost" (Verbindung unterbrochen)
- "Session Timeout" (Zeitüberschreitung bei der Sitzung)
- "VM Image Connected" (VM-Abbild verbunden)
- "VM Image Disconnected" (VM-Abbild getrennt)



- "CIM Update Started" (CIM-Aktualisierung gestartet)
- "CIM Update Completed" (CIM-Aktualisierung abgeschlossen)
- "CIM Connected" (CIM angeschlossen)
- "CIM Disconnected" (CIM getrennt)
- "Duplicate CIM Serial" (Doppelte CIM-Serie)
- "Forced User Logout" (Erzwungene Benutzerabmeldung)
- "Scan Started" (Scanvorgang gestartet)
- "Scan Stopped" (Scanvorgang angehalten)
- "User Added" (Benutzer hinzugefügt)
- "User Changed" (Benutzer geändert)
- "User Deleted" (Benutzer gelöscht)
- "Group Added" (Gruppe hinzugefügt)
- "Group Changed" (Gruppe geändert)
- "Group Deleted" (Gruppe geändert)

Netzwerk-Geschwindigkeitseinstellungen

Netzwerk-Geschwindigkeitseinstellung von LX							
Porteinstellung Netzwerkswitch		**Automatisch**	**1000/Voll**	**100/Voll**	**100/Halb**	**10/Voll**	**10/Halb**
	Automatisch	Höchste verfügbare Geschwindigkeit	1000/Voll	LX: 100/Voll Switch: 100/Halb	100/Halb	LX: 10/Voll Switch: 10/Halb	10/Halb
	1000/Voll	1000/Voll	1000/Voll	Keine Kommunikation	Keine Kommunikation	Keine Kommunikation	Keine Kommunikation
	100/Voll	LX: 100/Halb Switch: 100/Voll	LX: 100/Halb Switch: 100/Voll	100/Voll	LX: 100/Halb Switch: 100/Voll	Keine Kommunikation	Keine Kommunikation
	100/Halb	100/Halb	100/Halb	LX: 100/Voll Switch: 100/Halb	100/Halb	Keine Kommunikation	Keine Kommunikation
	10/Voll	LX: 10/Halb Switch: 10/Voll	Keine Kommunikation	Keine Kommunikation	Keine Kommunikation	10/Voll	LX: 10/Halb Switch: 10/Voll
	10/Halb	10/Halb	Keine Kommunikat	Keine Kommunikat	Keine Kommunikat	LX: 10/Voll	10/Halb

Netzwerk-Geschwindigkeitseinstellung von LX						
		ion	ion	ion	Switch: 10/Halb	

Legende:

(weißes Feld)	Funktioniert nicht wie erwartet
(grünes Feld)	Unterstützt
(türkises Feld)	Funktionen; nicht empfohlen
(rotes Feld)	NICHT von Ethernet-Spezifikationen unterstützt; Produkt kommuniziert, es treten allerdings Kollisionen auf.
(Feld mit dickem Rahmen)	Laut Ethernet-Spezifikation sollte hier "Keine Kommunikation" gelten, beachten Sie jedoch, dass das Verhalten des LX vom erwarteten Verhalten abweicht.

Hinweis: Um eine zuverlässige Netzwerkkommunikation zu erhalten, konfigurieren Sie LAN-Schnittstellengeschwindigkeit und Duplex für LX und den LAN-Switch auf den gleichen Wert. Konfigurieren Sie beispielsweise LX und den LAN-Switch auf "Autodetect" (Automatische Erkennung, empfohlen) oder stellen Sie sie auf ein(e) feste(s) Geschwindigkeit/Duplex wie 100MB/s/Voll.



Anhang B Aktualisieren des LDAP-Schemas

Hinweis: Die in diesem Kapitel beschriebenen Verfahren sollten nur von erfahrenen Benutzern durchgeführt werden.

In diesem Kapitel

Zurückgeben von Benutzergruppeninformationen

Verwenden Sie die Informationen in diesem Abschnitt, um Benutzergruppeninformationen zurückzugeben (und die Autorisierung zu unterstützen), sobald die Authentifizierung erfolgreich war.

Von LDAP/LDAPS

Wenn eine LDAP/LDAPS-Authentifizierung erfolgreich ist, bestimmt LX die Berechtigungen eines Benutzers anhand der Berechtigungen der Gruppe des Benutzers. Ihr Remote-LDAP-Server kann diese Benutzergruppennamen bereitstellen, indem er ein wie folgt benanntes Attribut zurückgibt:

rciusergroup attribute type: string

Dies erfordert ggf. eine Schemaerweiterung auf Ihrem LDAP/LDAPS-Server. Bitten Sie den Administrator des Authentifizierungsservers, dieses Attribut zu aktivieren.

Darüber hinaus wird für Microsoft® Active Directory® das Standard-LDAP-Attribut "memberOf" verwendet.



Von Microsoft Active Directory

Hinweis: Diese Aktualisierung sollte nur von einem erfahrenen Active Directory®-Administrator durchgeführt werden.

Die Rückgabe von Benutzergruppeninformationen von Microsoft® Active Directory für Windows 2000®-Server erfordert die Aktualisierung des LDAP-/LDAPS-Schemas. Weitere Informationen finden Sie in Ihrer Microsoft-Dokumentation.

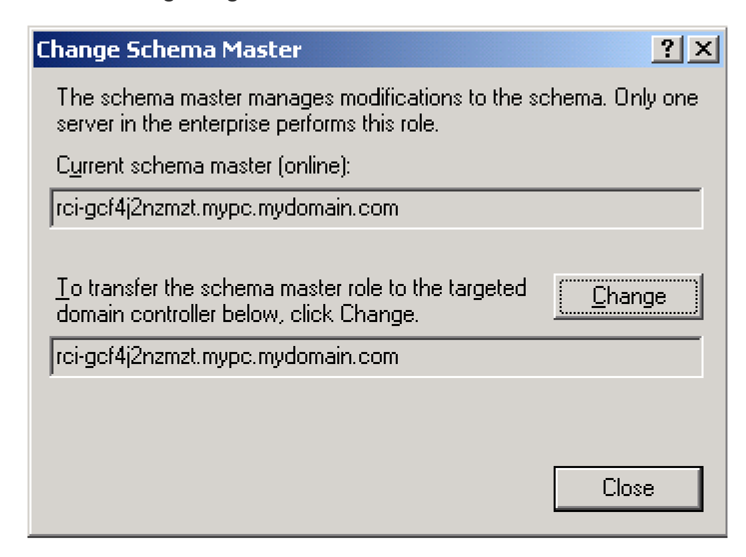
1. Installieren Sie das Schema-Plug-in für Active Directory. Entsprechende Anweisungen finden Sie in der Dokumentation für Microsoft Active Directory.
2. Starten Sie Active Directory Console und wählen Sie "Active Directory Schema" (Active Directory-Schema) aus.

Einstellen der Registrierung, um Schreibvorgänge im Schema zuzulassen

Um einem Domänencontroller das Schreiben im Schema zu erlauben, müssen Sie einen Registrierungseintrag erstellen, der Schemaaktualisierungen zulässt.

So lassen Sie Schreibvorgänge im Schema zu:

1. Klicken Sie mit der rechten Maustaste auf den Stammknoten des Active Directory® Schema im linken Fensterbereich, und wählen Sie "Operations Master" (Betriebsmaster) aus dem Kontextmenü aus. Das Dialogfeld "Change Schema Master" (Schemamaster ändern) wird angezeigt.



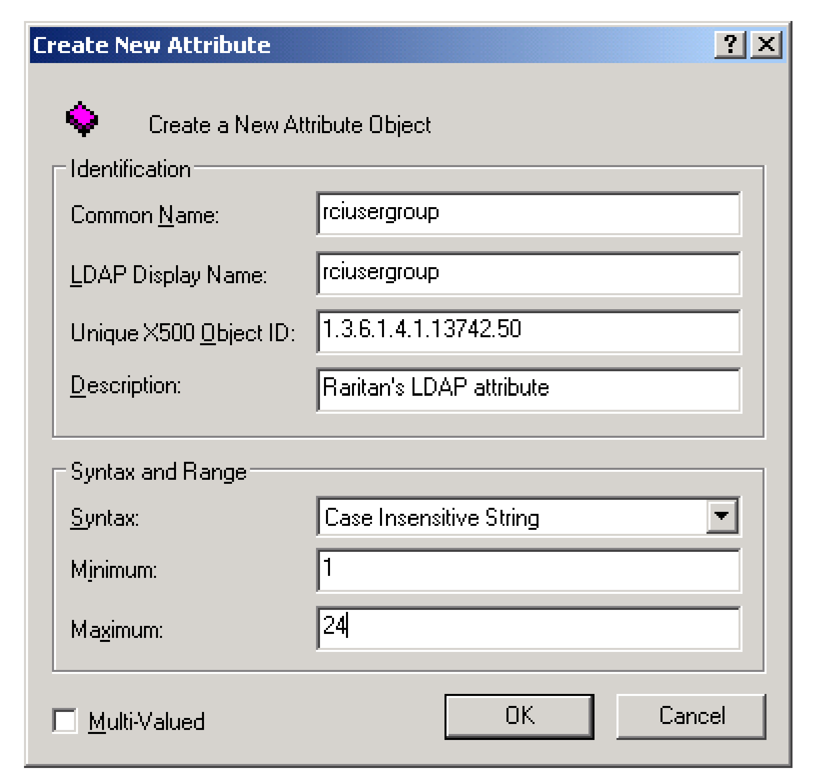


2. Aktivieren Sie das Kontrollkästchen "Schema can be modified on this Domain Controller" (Schema kann auf diesem Domänencontroller geändert werden). **Optional**
3. Klicken Sie auf OK.

Erstellen eines neuen Attributs

So erstellen Sie neue Attribute für die Klasse "rciusergroup":

1. Klicken Sie im linken Fensterabschnitt auf das +-Symbol vor Active Directory® Schema.
2. Klicken Sie im linken Fensterbereich mit der rechten Maustaste auf "Attributes" (Attribute).
3. Klicken Sie auf "New" (Neu) und wählen Sie "Attribute" (Attribut) aus. Klicken Sie im angezeigten Hinweisfenster auf "Continue" (Weiter). Das Dialogfeld "Create New Attribute" (Neues Attribut erstellen) wird geöffnet.



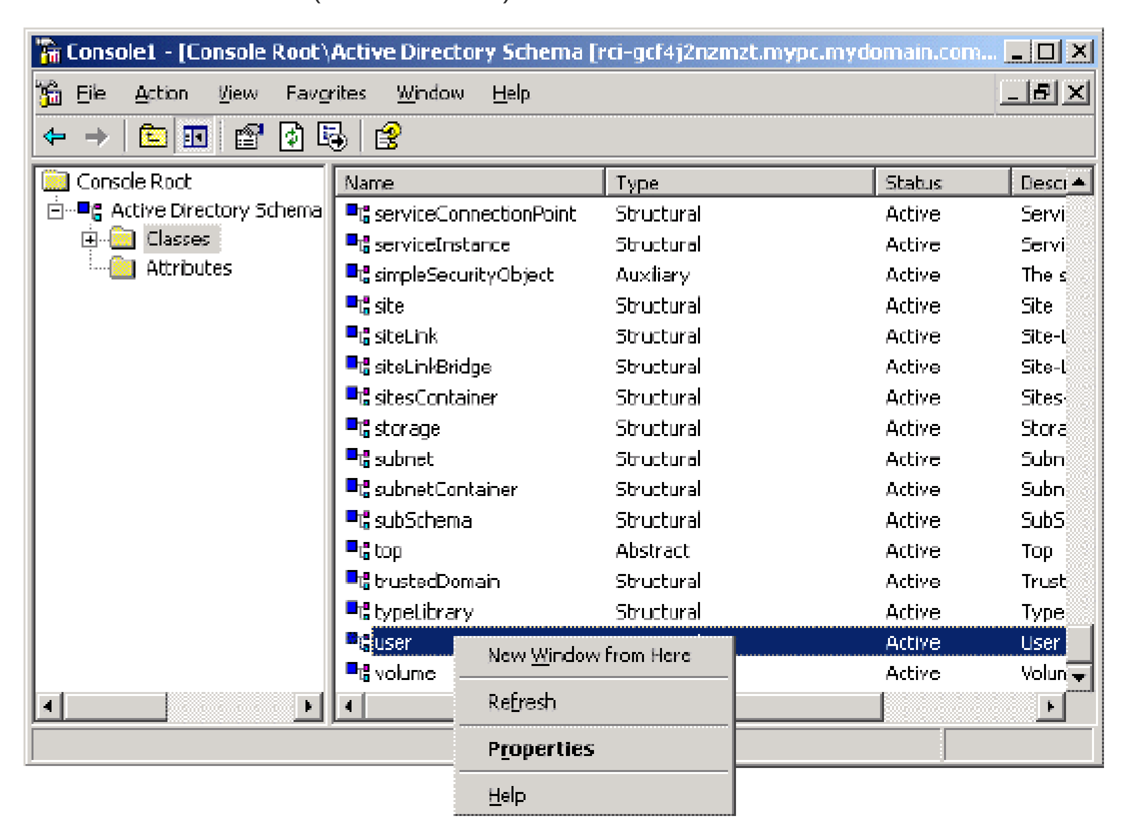
4. Geben Sie im Feld "Common Name" (Allgemeiner Name) den Wert *rciusergroup* ein.
5. Geben Sie im Feld "LDAP Display Name" (LDAP-Anzeigename) den Wert *rciusergroup* ein.

6. Geben Sie im Feld "Unique x5000 Object ID" (Eindeutige X500-OID) den Wert *1.3.6.1.4.1.13742.50* ein.
7. Geben Sie eine aussagekräftige Beschreibung im Feld "Description" (Beschreibung) ein.
8. Klicken Sie auf die Dropdownliste "Syntax" und wählen Sie "Case Insensitive String" (Groß-/Kleinschreibung nicht beachten) aus.
9. Geben Sie im Feld "Minimum" den Wert *1* ein.
10. Geben Sie im Feld "Maximum" den Wert *24* ein.
11. Klicken Sie zum Erstellen des neuen Attributs auf OK.

Hinzufügen von Attributen zur Klasse

So fügen Sie der Klasse Attribute hinzu:

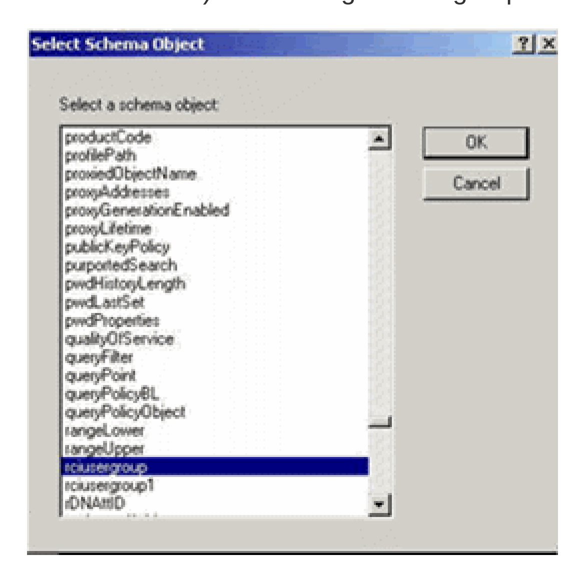
1. Klicken Sie im linken Fensterbereich auf "Classes" (Klassen).
2. Suchen Sie im rechten Fensterbereich den Wert "User Class" (Benutzerklasse) und klicken Sie mit der rechten Maustaste darauf.



3. Wählen Sie "Properties" (Eigenschaften) aus dem Kontextmenü. Das Dialogfeld "User Properties" (Benutzereigenschaften) wird geöffnet.



4. Klicken Sie auf die Registerkarte "Attributes" (Attribute), um diese zu öffnen.
5. Klicken Sie auf "Add" (Hinzufügen).
6. Wählen Sie in der Liste "Select Schema Object" (Schemaobjekt auswählen) den Eintrag "rciusergroup" aus.



7. Klicken Sie im Dialogfeld "Select Schema Object" (Schemaobjekt auswählen) auf OK.
8. Klicken Sie im Dialogfeld "User Properties" (Benutzereigenschaften) auf OK.

Aktualisieren des Schemacache

▶ So aktualisieren Sie den Schemacache:

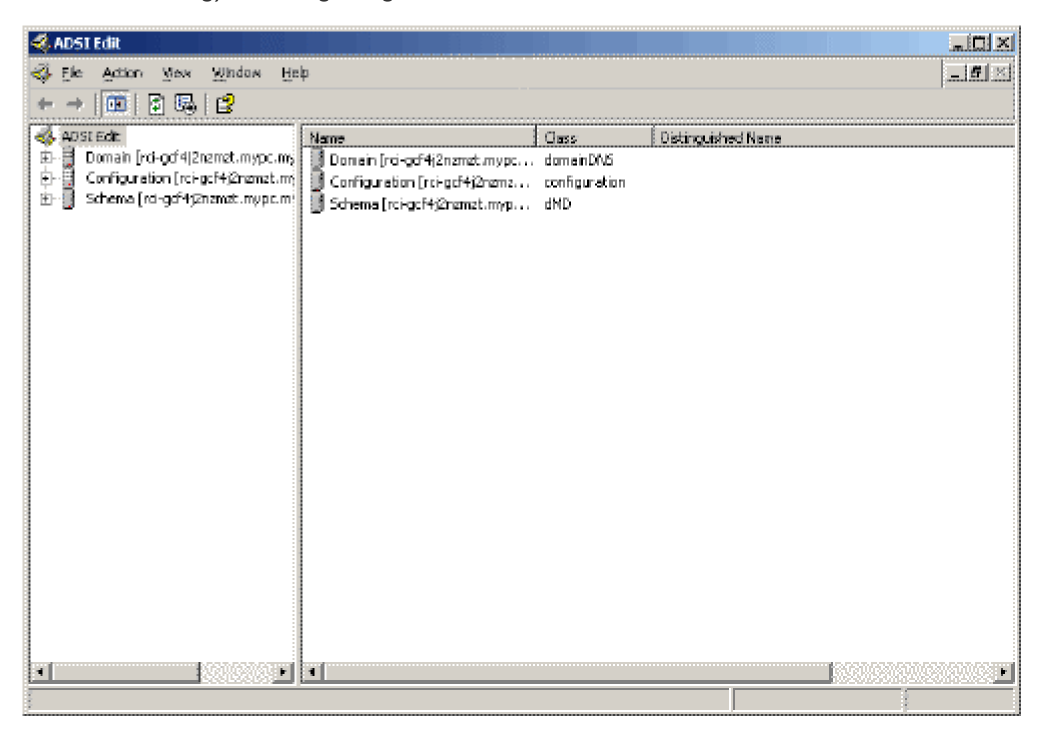
1. Klicken Sie im linken Fensterbereich mit der rechten Maustaste auf "Active Directory® Schema", und wählen Sie "Reload the Schema" (Schema neu laden) aus.
2. Minimieren Sie die Active Directory-Schema-MMC-Konsole (Microsoft® Management Console).

Bearbeiten von rciusergroup-Attributen für Benutzermitglieder

Verwenden Sie zum Ausführen des Active Directory®-Skripts auf einem Windows 2003®-Server das von Microsoft® bereitgestellte Skript (verfügbar auf der Windows 2003-Serverinstallations-CD). Diese Skripts werden bei der Installation von Microsoft® Windows 2003 mit installiert. ADSI (Active Directory Service Interface) fungiert hierbei als Low-Level-Editor für Active Directory und ermöglicht so das Durchführen allgemeiner Verwaltungsaufgaben wie Hinzufügen, Löschen und Verschieben von Objekten mit einem Verzeichnisdienst.

So bearbeiten Sie die einzelnen Benutzerattribute innerhalb der Gruppe "rciusergroup":

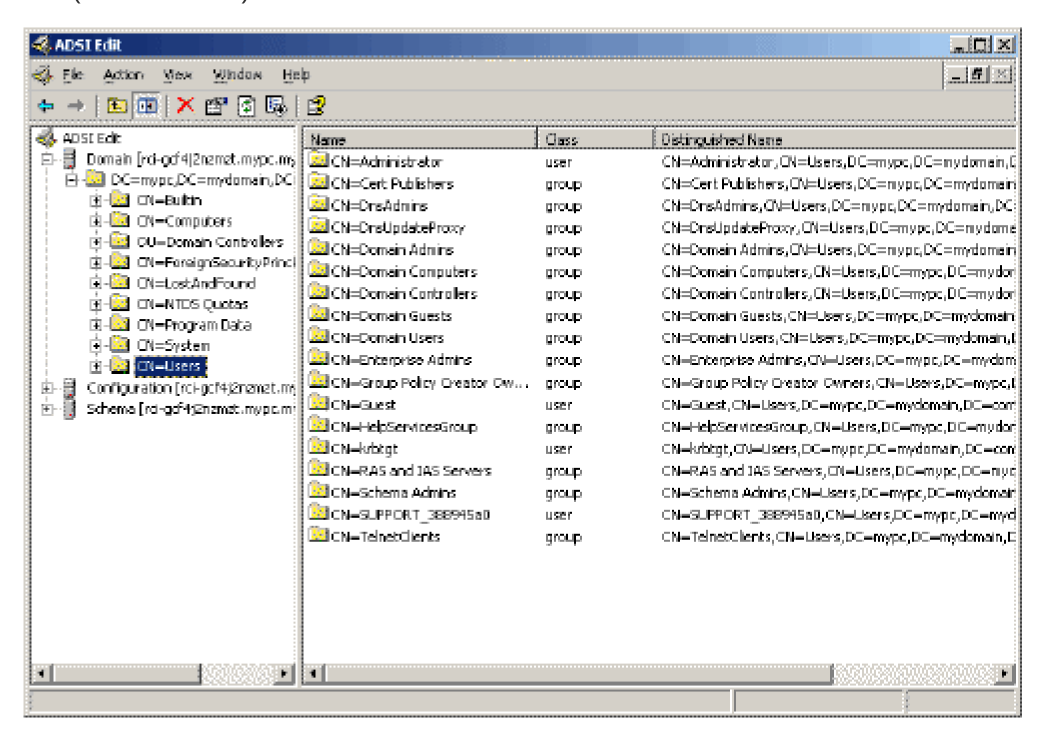
1. Wählen Sie auf der Installations-CD "Support" > "Tools" aus.
2. Doppelklicken Sie zur Installation der Support-Tools auf "SUPTOOLS.MSI".
3. Wechseln Sie zum Installationsverzeichnis der Support-Tools. Führen Sie "adsiedit.msc" aus. Das Fenster "ADSI Edit" (ADSI-Bearbeitung) wird angezeigt.



4. Öffnen Sie die Domäne.

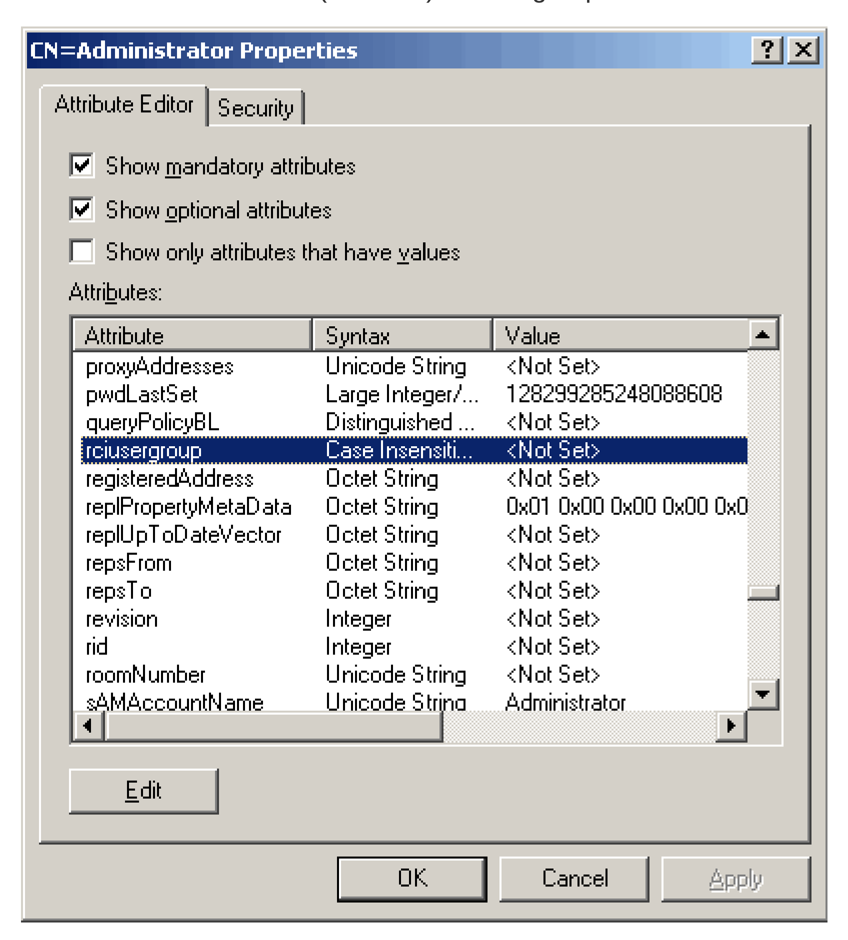


5. Klicken Sie im linken Fensterbereich auf den Ordner "CN=Users" (CN=Benutzer).

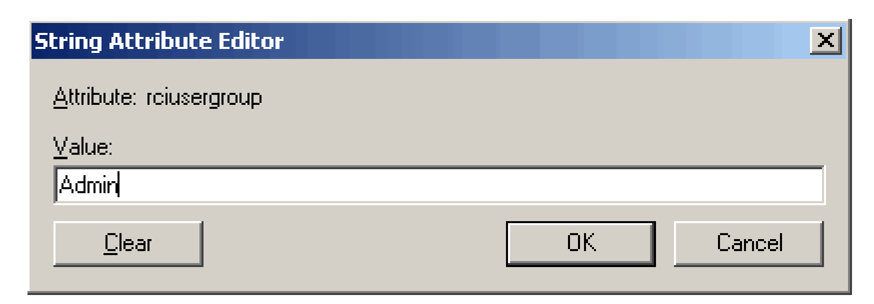


6. Navigieren Sie im rechten Fensterbereich zu dem Namen des Benutzers, dessen Eigenschaften geändert werden sollen. Klicken Sie mit der rechten Maustaste auf den Benutzernamen, und wählen Sie "Properties" (Eigenschaften) aus dem Kontextmenü aus.

7. Klicken Sie auf die Registerkarte "Attribute Editor" (Attributeditor), um sie anzuzeigen, wenn sie noch nicht geöffnet ist. Wählen Sie in der Liste "Attributes" (Attribute) "rciusergroup" aus.



8. Klicken Sie auf "Edit" (Bearbeiten). Das Dialogfeld "String Attribute Editor" (Attributeditor für Zeichenfolgen) wird angezeigt.
9. Geben Sie die Benutzergruppe (erstellt in LX) in das Feld "Edit Attribute" (Attribut bearbeiten) ein. Klicken Sie auf OK.





Anhang C Wichtige Hinweise

In diesem Kapitel

Überblick

Dieser Abschnitt enthält wichtige Hinweise zur Verwendung des LX. Zukünftige Aktualisierungen werden dokumentiert und sind online über den Link "Help" (Hilfe) auf der Benutzeroberfläche der LX-Remotekonsole verfügbar.

Hinweis: Einige Kapitel in diesem Abschnitt beziehen sich auf andere Geräte von Raritan, da diese Informationen auf verschiedene Geräte zutreffen.

Java Runtime Environment (JRE)

Wichtig: Sie sollten die Zwischenspeicherung für Java™ deaktivieren und den Java-Cache leeren. Weitere Informationen finden Sie in der Java-Dokumentation oder im Benutzerhandbuch "KVM and Serial Access Clients Guide".

Für die Remotekonsole LX, KX II, KX II-101 und KX II-101-V2 und den MPC ist Java Runtime Environment™ (JRE™) erforderlich, da die Remotekonsole die Java-Version überprüft. Falls die Version falsch oder veraltet ist, werden Sie dazu aufgefordert, eine kompatible Version herunterzuladen.

Raritan empfiehlt zur Gewährleistung einer optimalen Leistung die Verwendung von JRE Version 1.6, die Remotekonsole und der MPC funktionieren jedoch auch mit JRE Version 1.6.x oder höher (mit Ausnahme von 1.6.2).

Hinweis: Damit mehrsprachige Tastaturen in der Remotekonsole LX, KX II, KX II-101 und KX II-101-V2 (Virtual KVM Client) funktionieren, müssen Sie die mehrsprachige Version von JRE installieren.

Hinweise zur Unterstützung von IPv6

Java

Java™ 1.6 unterstützt IPv6 bei folgenden Produkten:

- Solaris™ 10 (und höher)
- Linux® Kernel 2.1.2 (und höher)/RedHat 6.1 (und höher)

Java 5.0 und höher unterstützen IPv6 bei folgenden Produkten:

- Solaris 10 (und höher)
- Linux Kernel 2.1.2 (und höher), Kernel 2.4.0 (und höher) wird für bessere IPv6-Unterstützung empfohlen.
- Betriebssysteme Windows XP® SP1 und Windows 2003®, Windows Vista®

Die folgenden IPv6-Konfigurationen werden *nicht* von Java unterstützt:

- J2SE 1.4 unterstützt kein IPv6 auf Microsoft® Windows®.

Linux

- Es wird empfohlen, bei Nutzung von IPv6 Linux Kernel 2.4.0 oder höher zu verwenden.
- Ein IPv6-aktivierter Kernel muss installiert werden, oder der Kernel muss mit aktivierten IPv6-Optionen wiederhergestellt werden.
- Bei der Verwendung von IPv6 und Linux müssen außerdem einige Netzwerkdienste installiert werden. Weitere Informationen finden Sie unter http://www.bieringer.de/linux/IPv6/IPv6-HOWTO/IPv6-HOWTO.html.

Windows

- Windows XP- und Windows 2003-Benutzer müssen Microsoft Service Pack für IPv6 installieren, um IPv6 zu aktivieren.

Mac Leopard

- Die KX II-Version 2.0.20 unterstützt für Mac® Leopard® kein IPv6.

Samba

- Bei der Verwendung von Samba zusammen mit virtuellen Medien wird kein IPv6 unterstützt.



Tastaturen

Tastaturen (nicht USA)

Französische Tastatur

Zirkumflexzeichen (nur Linux®-Clients)

Virtual KVM Client und Multi-Platform-Client (MPC) unterstützen bei Verwendung einer französischen Tastatur mit Linux-Clients nicht die Tastenkombination "Alt Gr+9" für das Zirkumflexzeichen (^).

So stellen Sie das Zirkumflexzeichen dar:

Drücken Sie auf einer französischen Tastatur die ^-Taste (rechts neben der P-Taste) und unmittelbar danach die Leertaste.

Alternativ können Sie ein Makro erstellen, das aus folgender Befehlsabfolge besteht:

1. Rechte Alt-Taste drücken
2. Taste "9" drücken
3. Taste "9" loslassen
4. Rechte Alt-Taste loslassen

Hinweis: Dieser Vorgang kann bei der Verwendung des Zirkumflexzeichens mit anderen Buchstaben (als Akzent über Vokalen) nicht durchgeführt werden. In diesem Fall verwenden Sie die ^-Taste (rechts neben der P-Taste) auf französischen Tastaturen.

Akzentzeichen (nur Windows XP®-Betriebssystem-Clients)

Im Virtual KVM Client und Multi-Platform-Client wird bei Verwendung der Tastenkombination "Alt Gr+7" das Akzentzeichen zweimal dargestellt, wenn eine französische Tastatur für Windows XP-Clients verwendet wird.

Hinweis: Dies trifft nicht auf Linus-Clients zu.

Nummernblock

Im Virtual KVM Client und Multi-Platform-Client werden die Zeichen auf dem Nummernblock bei französischen Tastaturen wie folgt dargestellt:

Zeichen auf dem Nummernblock	Dargestellt als
/	;

.	;

Tilde

Im Virtual KVM Client und Multi-Platform-Client wird bei Verwendung einer französischen Tastatur durch die Tastenkombination "Alt Gr+2" nicht die Tilde (~) angezeigt.

So stellen Sie die Tilde dar:

Erstellen Sie mit der folgenden Befehlsabfolge ein Makro:

- Rechte Alt-Taste drücken
- Taste "2" drücken
- Taste "2" loslassen
- Rechte Alt-Taste loslassen

Einstellungen der Tastatursprache (Fedora Linux-Clients)

Da mit der Sun™-JRE™ auf einem Linux®-Betriebssystem Probleme bei der korrekten Erzeugung von KeyEvents (Tastenereignissen) für fremdsprachige Tastaturen auftreten, die mithilfe der Systemeinstellungen konfiguriert wurden, empfiehlt Raritan die Konfiguration fremdsprachiger Tastaturen mithilfe der in der folgenden Tabelle beschriebenen Methoden.

Sprache	Konfigurationsmethode
USA/Int.	Standard
Britisches Englisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]
Französisch	Keyboard Indicator (Tastaturanzeige)
Deutsch (Deutschland)	Keyboard Indicator (Tastaturanzeige)
Ungarisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]
Spanisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]
Deutsch (Schweiz)	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]
Norwegisch	Keyboard Indicator (Tastaturanzeige)
Schwedisch	Keyboard Indicator (Tastaturanzeige)
Dänisch	Keyboard Indicator (Tastaturanzeige)
Japanisch	System Settings (Control Center)



Sprache	Konfigurationsmethode
USA/Int.	Standard
	[Systemeinstellungen (Steuerzentrale)]
Koreanisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]
Slowenisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]
Italienisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]
Portugiesisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]

Hinweis: Die Tastaturanzeige sollte bei Linux-Systemen, die Gnome als Desktopumgebung nutzen, verwendet werden.

Bei Verwendung einer ungarischen Tastatur mit einem Linux-Client werden die lateinischen Buchstaben "U" mit Doppelakut und "O" mit Doppelakut nur dargestellt, wenn JRE 1.6 verwendet wird.

Es gibt mehrere Methoden, die Einstellungen der Tastatursprache bei Fedora® Linux-Clients festzulegen. Die folgende Methode muss angewendet werden, um die Tasten für den Virtual KVM Client und den Multi-Platform Client (MPC) korrekt zuzuordnen.

► So legen Sie die Tastatursprache unter "System Settings" (Systemeinstellungen) fest:

1. Wählen Sie in der Symbolleiste "System" > "Preferences" > "Keyboard" (System > Einstellungen > Tastatur) aus.
2. Öffnen Sie die Registerkarte "Layouts" (Tastatursprache).
3. Wählen Sie die entsprechende Sprache aus oder fügen Sie sie hinzu.
4. Klicken Sie auf "Close" (Schließen).

► So legen Sie die Tastatursprache unter "Keyboard Indicator" (Tastaturanzeige) fest:

1. Klicken Sie mit der rechten Maustaste auf die Taskleiste und wählen Sie "Add to Panel" (Zu Panel hinzufügen) aus.
2. Klicken Sie im Dialogfeld "Add to Panel" (Zu Panel hinzufügen) mit der rechten Maustaste auf "Keyboard Indicator" (Tastaturanzeige) und wählen Sie aus dem Kontextmenü "Open Keyboard Preferences" (Tastatureinstellungen öffnen) aus.
3. Klicken Sie im Dialogfeld "Keyboard Preferences" (Tastatureinstellungen) auf die Registerkarte "Layouts" (Tastatursprache).

4. Fügen Sie Sprachen wie gewünscht hinzu oder löschen Sie sie.

Macintosh-Tastatur

Wenn Macintosh® als Client verwendet wird, funktionieren die folgenden Tasten auf der Mac®-Tastatur unter Verwendung von Java™ Runtime Environment (JRE™) nicht.

- F9
- F10
- F11
- F14
- F15
- Volume Up (Lautstärke höher)
- Volume Down (Lautstärke niedriger)
- Mute (Stummschaltung)
- Eject (Ausgabe)

Deshalb können diese Tasten bei Verwendung von Virtual KVM Client und Multi-Platform Client (MPC) zusammen mit einer Mac-Clienttastatur nicht verwendet werden.

Fedora

Beheben von Fokusproblemen bei Fedora Core

Bei Verwendung des Multi-Platform-Client (MPC) kann es vorkommen, dass Sie sich nicht am LX-, KX II- oder KSX II-Gerät anmelden oder nicht auf den KVM-Zielserver zugreifen können (Windows®, SUSE usw.). Außerdem wird durch Drücken der Tastenkombination "Strg+Alt+M" möglicherweise nicht das Zugriffstastenmenü aufgerufen. Diese Situation tritt bei der folgenden Clientkonfiguration auf: Fedora® Core 6 und Firefox® 1.5 oder 2.0.

Durch Tests wurde festgestellt, dass die Fensterfokussierungsprobleme bei Fedora Core 6 durch die Installation von libXp behoben werden können. Bei den von Raritan durchgeführten Tests mit libXp-1.0.0.8.i386.rpm konnten alle Probleme der Tastaturfokussierung und mit Popup-Menüs behoben werden.

Hinweis: libXp ist auch für den SeaMonkey-Browser (ehemals Mozilla®) erforderlich, damit dieser mit dem Java™-Plug-in funktioniert.



Mauszeigersynchronisierung (Fedora)

Wenn bei Verwendung von Fedora® 7 eine Verbindung zu einem Zielserver über den Zwei-Cursor-Modus besteht und die Synchronisierung der lokalen und Ziel-Cursor nach einiger Zeit unterbrochen wird, kann durch das Ändern des Mausmodus von "Intelligent" in "Standard" oder umgekehrt die Synchronisierung verbessert werden. Der Ein-Cursor-Modus ermöglicht ebenfalls eine verbesserte Steuerung.

So synchronisieren Sie die Cursor erneut:

- Verwenden Sie die Option "Synchronize Mouse" (Maus synchronisieren) im Virtual KVM Client.

Lösen von Problemen mit dem Einfrieren von Firefox bei der Benutzung von Fedora

Wenn Sie Firefox® verwenden und einen Fedora®-Server nutzen, ist es möglich, dass Firefox beim Öffnen einfriert. Um dieses Problem zu lösen, installieren Sie das Java™-Plug-in libnpjp2.so auf dem Server.

Videomodi und Auflösungen

Videomodi für SUSE/VESA

Das SuSE X.org-Konfigurationstool "SaX2" erzeugt Videomodi mithilfe von Modeline-Einträgen in der X.org-Konfigurationsdatei. Diese Videomodi stimmen nicht exakt mit der Zeitabstimmung des VESA-Videomodus überein (auch wenn ein VESA-Monitor ausgewählt wurde). LX verwendet die Zeitabstimmung des VESA-Videomodus für die ordnungsgemäße Synchronisierung und verlässt sich auf deren Richtigkeit. Diese Unstimmigkeit kann zu schwarzen Rändern, fehlenden Abschnitten im Bild und Rauschen führen.

So konfigurieren Sie die SUSE-Videoanzeige:

1. Die erzeugte Konfigurationsdatei "/etc/X11/xorg.conf" enthält einen Abschnitt zum Monitor mit einer Option, die als "UseModes" bezeichnet wird, z. B.
   UseModes "Modes[0]".
2. Kommentieren Sie diese Zeile aus (mit #) oder löschen Sie sie vollständig.
3. Starten Sie den X-Server neu.

Durch diese Änderung wird die interne Zeitabstimmung für den Videomodus des X-Servers verwendet, der exakt mit der Zeitabstimmung des VESA-Videomodus übereinstimmt und so zur gewünschten Videoanzeige auf LX führt.

Unterstützte Videoauflösungen, die nicht angezeigt werden

Wenn Sie ein CIM verwenden, gibt es einige Videoauflösungen, wie unter Unterstützte Videoauflösungen aufgelistet, die nicht standardmäßig zur Auswahl stehen.

So können Sie alle verfügbaren Videoauflösungen anzeigen:

1. Stecken Sie den Monitor ein.
2. Stecken Sie als nächsten Schritt den Monitor wieder aus und das CIM ein. Jetzt sind alle Videoauflösungen verfügbar und können verwendet werden.

VM-CIMs und DL360 USB-Ports

HP® DL360-Server verfügen über einen USB-Port auf der Rückseite des Geräts und einen weiteren auf der Vorderseite. Mit DL360 können nicht beide Ports gleichzeitig verwendet werden. Deshalb kann ein duales VM-CIM auf DL360-Servern nicht verwendet werden.

Sie können jedoch einen USB2-Hub an den USB-Port auf der Rückseite des Geräts angeschlossen werden, an den wiederum ein duales VM-CIM angeschlossen werden kann.

MCUTP

Die Seriennummer und der CIM-Name, die auf dem MCUTP verfügbar sind, werden nicht im Gerät gespeichert. Deshalb unterscheidet sich die Funktionsweise von MCUTP-Ports im Vergleich zu anderen. Dies gilt speziell für folgende Merkmale:

- Der Name wird nicht im CIM gespeichert. Beim Portnamen handelt es sich um eine Bezeichnung im Zusammenhang mit dem Port (vorausgesetzt der Porttyp ändert sich nicht, da ein anderer CIM-Typ angeschlossen wird).
- Stromzuordnungen sind bei diesem Porttyp nicht möglich
- Zieleinstellungen sind bei diesem Porttyp nicht möglich
- Die Seriennummer wird auf Anzeigen mit der CIM-Seriennummer oder Protokolleinträgen als 'N/A' angezeigt
- Bei diesem Porttyp sind keine Zuordnungen zu Portgruppen möglich
- Bei diesem Porttyp sind keine Zuordnungen zu Verbindungsskripts möglich



Virtual Media (Virtuelle Medien)

Virtuelle Medien über den VKC und den AKC in einer Windows-Umgebung

Die Berechtigungen für den Systemadministrator und Standardbenutzer unter dem Betriebssystem Windows XP® unterscheiden sich von den Berechtigungen unter den Betriebssystemen Windows Vista® und Windows 7®.

Ist die "User Access Control (UAC)" (Benutzerzugriffssteuerung) unter Windows Vista oder Windows 7 aktiviert, so bietet diese die Berechtigungen der niedrigsten Stufe, die ein Benutzer für eine Anwendung benötigt. Beispielsweise ist die Option "Run as Administrator" (Als Administrator ausführen) für Internet Explorer® verfügbar, um Benutzern die Ausführung spezieller Aufgaben auf Administratorebene zu gestatten. Diese Berechtigung würde sonst nicht bestehen, selbst wenn der Benutzer über ein Administratorkonto verfügt.

Diese beiden Funktionen wirken sich darauf aus, auf welchen Typ virtueller Medien von Benutzern über den Virtual KVM Client (VKC) und den Active KVM Client (AKC) zugegriffen werden kann. Weitere Informationen zu diesen Funktionen und deren Verwendung finden Sie in Ihrer Microsoft®-Hilfe.

Im Folgenden finden Sie eine Liste mit Typen virtueller Medien, auf die über den VKC und den AKC aus einer Windows-Umgebung zugegriffen werden kann. Die Funktionen sind nach Client-Funktionen und Funktionen der virtuellen Medien aufgeteilt, die den einzelnen Windows-Benutzerfunktionen zugewiesen sind.

Windows XP

Wenn Sie den VKC und den AKC in einer Windows XP-Umgebung ausführen, müssen Benutzer über Administratorrechte verfügen, um auf andere Medientypen als CD-ROM-Verbindungen, ISO-Dateien und ISO-Abbilder zugreifen zu können.

Windows Vista und Windows 7

Wenn Sie den VKC und den AKC in einer Windows Vista- oder Windows 7-Umgebung bei aktivierter UAC ausführen, kann, je nach Windows-Benutzerfunktion, auf die folgenden virtuellen Medientypen zugegriffen werden.

Client	Administrator	Standard-Benutzer

Client	Administrator	Standard-Benutzer
AKC und VKC	Zugriff auf: • Fest installierte Laufwerke und deren Partitionen • Wechsellaufwerke • CD-/DVD-Laufwerke • ISO-Abbilder • Remote-ISO-Abbilder	Zugriff auf: • Wechsellaufwerke • CD-/DVD-Laufwerke • ISO-Abbilder • Remote-ISO-Abbilder

Laufwerkpartitionen

- Die folgenden Einschränkungen für Laufwerkpartitionen gelten für verschiedene Betriebssysteme:
  - Windows- und Mac-Ziele können keine unter Linux formatierten Partitionen lesen.
  - Windows® und Linux® können keine unter Mac formatierten Partitionen lesen.
  - Von Linux werden nur Windows FAT-Partitionen unterstützt.
  - Mac unterstützt Windows FAT und NTFS.

  Mac-Benutzer müssen alle bereits installierten Geräte deinstallieren, um eine Verbindung mit einem Zielserver herzustellen. Verwenden Sie den Befehl ">diskutil umount /dev/disk1s1", um das Gerät zu deinstallieren, und "diskutil mount /dev/disk1s1", um es erneut zu installieren.

Virtuelle Medien werden nach dem Hinzufügen von Dateien nicht aktualisiert

Nach der Installation eines virtuellen Medienlaufwerks werden dem Laufwerk hinzugefügte Dateien möglicherweise nicht unmittelbar auf dem Zielserver angezeigt. Trennen Sie die virtuelle Medienverbindung und stellen Sie sie erneut her.

Aktive Systempartitionen

Sie können keine aktiven Systempartitionen von einem Mac- oder Linux-Client bereitstellen.

Vor dem Herstellen einer virtuellen Medienverbindung muss die Bereitstellung von Linux Ext3/4-Laufwerkpartitionen mit dem Befehl "umount /dev/<Gerätekennzeichnung>" aufgehoben werden.



Laufwerkpartitionen

Die folgenden Einschränkungen für Laufwerkpartitionen gelten für verschiedene Betriebssysteme:

- Windows- und Mac-Ziele können keine unter Linux formatierten Partitionen lesen.
- Windows® und Linux® können keine unter Mac formatierten Partitionen lesen.
- Von Linux werden nur Windows FAT-Partitionen unterstützt.
- Mac unterstützt Windows FAT und NTFS.
- Mac-Benutzer müssen alle bereits installierten Geräte deinstallieren, um eine Verbindung mit einem Zielserver herzustellen. Verwenden Sie den Befehl ">diskutil umount /dev/disk1s1", um das Gerät zu deinstallieren, und "diskutil mount /dev/disk1s1", um es erneut zu installieren.

Zwei Listeneinträge für das Linux-Laufwerk für virtuelle Medien

Für den KX II 2.4.0 (und höher) und LX 2.4.5 (und höher) werden die Laufwerke für Benutzer, die bei Linux™-Clients als Stammbenutzer angemeldet sind, die Laufwerke in der Dropdownliste "Local Drive" (Lokales Laufwerk) zweimal aufgeführt. Beispielsweise werden "eg /dev/sdc" und "eg /dev/sdc1" angezeigt, wobei das erste Laufwerk der Bootsektor und das zweite Laufwerk die erste Partition auf der Festplatte ist.

Unter Mac und Linux gesperrte, zugeordnete Laufwerke

Zugeordnete Laufwerke von Mac®- und Linux®-Clients sind nicht gesperrt, wenn sie auf verbundenen Zielen bereitgestellt werden. Dies gilt nur für den KX II 2.4.0 (und höher) und LX 2.4.5 (und höher), die Unterstützung für Mac und Linux bieten.

Zugriff auf virtuelle Medien auf einem Windows 2000 Server mithilfe eines D2CIM-VUSB

Der Zugriff auf virtuelle Medien auf einem lokalen Laufwerk auf einem Windows 2000® Server ist mit D2CIM-VUSB nicht möglich.

Bootzeit des Ziel-BIOS bei Verwendung von virtuellen Medien

Das BIOS bestimmter Zielgeräte benötigt möglicherweise mehr Zeit zum Hochfahren, wenn virtuelle Medien auf dem Zielgerät installiert sind.

So verkürzen Sie die Bootzeit:

1. Schließen Sie den Virtual KVM Client, sodass die virtuellen Medienlaufwerke vollständig freigegeben werden.

2. Starten Sie das Zielgerät neu.

Fehler bei Hochgeschwindigkeitsverbindungen mit virtuellen Medien

Unter bestimmten Umständen kann es erforderlich sein, die Verbindungsgeschwindigkeit "Use Full Speed for Virtual Media CIM" (Volle Geschwindigkeit für virtuelles Medien-CIM verwenden) auszuwählen. Zum Beispiel bei Problemen des Ziels mit der USB-Hochgeschwindigkeitsverbindung oder wenn beim Ziel USB-Protokollfehler aufgrund von Signalstörungen, zusätzlichen Anschlüssen und Kabeln auftreten..

CIMs

Windows-3-Tasten-Maus auf Linux-Zielgeräten

Wenn Sie auf einem Windows®-Client eine 3-Tasten-Maus verwenden und eine Verbindung zu einem Linux®-Zielgerät herstellen, wird die linke Maustaste möglicherweise der mittleren Taste der 3-Tasten-Maus des Windows-Client zugeordnet.

Composite-USB-Geräteverhalten bei virtuellen Medien auf Windows 2000

Das Betriebssystem Windows 2000® unterstützt Composite-USB-Geräte (z. B. D2CIM-VUSB von Raritan) nicht im gleichen Maße wie Non-Composite-USB-Geräte.

Aus diesem Grund wird das Symbol zum sicheren Entfernen der Hardware im Infobereich der Taskleiste bei Laufwerken, die von D2CIM-VUSB zugeordnet wurden, nicht angezeigt, und beim Verbinden des Geräts wird möglicherweise eine Warnmeldung angezeigt. Es wurden von Raritan keine daraus resultierenden Probleme oder Fehler festgestellt.



MCUTP-CIM-Verhalten

Da die CIM-Seriennummer bzw. der CIM-Name auf dem MCUTP nicht gespeichert werden, unterscheidet sich die Funktionsweise von Ports dieses Typs von anderen CIMs. Dies gilt speziell für folgende Merkmale:

- Der CIM-Name wird nicht gespeichert
- Beim Portnamen handelt es sich um eine Bezeichnung im Zusammenhang mit dem Port (vorausgesetzt der Porttyp ändert sich nicht, da ein anderer CIM-Typ angeschlossen wird)
- Zieleinstellungen sind bei diesem Porttyp nicht möglich
- Die Seriennummer wird auf Anzeigen mit der CIM-Seriennummer oder Protokolleinträgen als 'N/A' angezeigt

Anhang D Häufig gestellte Fragen

In diesem Kapitel



Kapitel 12

LX-FAQs

Frage	Antwort
Was ist Dominion LX?	Bei Dominion LX handelt es sich um eine Reihe von ökonomischen KVM-über-IP-Switches mit Einzelstromversorgung, einem LAN-Anschluss und virtuellen Medien. Sie eignen sich für kleine und mittelständische Unternehmen mit weniger als 75 Servern, sie ermöglichen Zugriff auf BIOS-Ebene sowie die IP-Steuerung von 8 bzw. 16 Servern mit Zugriffsmöglichkeiten für einen oder zwei Remotebenutzer.
Wie lässt sich der typische LX-Kunde beschreiben?	Der typische Kunde, in der Regel ein IT-Administrator oder Softwareentwickler/-tester, arbeitet für ein kleines oder mittelständisches Unternehmen, das einen äußerst leistungsstarken KVM-über-IP-Remotezugriff zu einem günstigen Preis benötigt. LX-Kunden legen Wert auf produktivitätssteigernde Funktionen wie virtuelle Medien, den Mausmodus "Absolute Mouse Synchronization™" und gängige Benutzeroberflächen für Remote- und lokalen Zugriff.
Was ist das Besondere an Dominion LX?	LX bietet einen äußerst leistungsstarken, qualitativ hochwertigen KVM-über-IP-Switch zu einem günstigen Preis. Im Gegensatz zu anderen Produkten in dieser Preisklasse werden produktivitätssteigernde Funktionen wie virtuelle Medien, der Mausmodus "Absolute Mouse Synchronization™" und gängige Oberflächen für Remote- und lokale Benutzer unterstützt.
Welche Arten von IT-Geräten kann LX verwalten?	LX eignet sich für Computer und seriell gesteuerte Geräte, einschließlich Computerserver und -geräte, Telekommunikations- und Netzwerkgeräte.
Welche Funktionen zur Remoteverwaltung werden unterstützt?	Dominion LX ermöglicht zuverlässige Out-of-band-Remoteverwaltung. Dazu gehört die KVM-über-IP-Steuerung auf BIOS-Ebene, der Remotezugriff auf virtuelle Medien und der optionale Modemzugriff. LX ermöglicht unabhängig vom Status des Zielgeräts jederzeit und überall Remoteverwaltung. Sie können auf BIOS-Ebene zugreifen, Hardwarediagnosen durchführen, einen abgestürzten Server neu starten, Software von DVDs installieren und sogar ein neues Serverabbild erstellen – und das alles von einem Remotestandort aus.
Wie schneidet Dominion LX im Vergleich zu Produkten anderer Anbieter ab?	Andere Anbieter stellen in der Regel einfache KVM-über-IP-Switches mit eingeschränkten Funktionen und einer Benutzeroberfläche mit Bildschirmanzeige der älteren Generation zur Verfügung. Die Produkte anderer Anbieter sind nicht mit den Standardfunktionen wie virtuelle Medien, dem Mausmodus "Absolute Mouse Synchronization", einer Remote-Videoauflösung von 1920x1080 und standardmäßigen Sicherheitsfunktionen ausgestattet.

Frage	Antwort
Welche Vorteile bietet LX?	Einen qualitativ hochwertigen KVM-über-IP-Switch zu einem günstigen Preis für das IT- und Entwicklungspersonal kleiner und mittelständischer Unternehmen. Die Vorteile von LX bestehen im Remotezugriff und der Steuerung von Servern und anderen IT-Geräten - und zwar jederzeit und überall. LX-Kunden profitieren von: • Reduzierten Reisekosten • Erhöhter Produktivität • Reduzierter mittlerer Reparaturdauer • Qualitativ hochwertigeren Services
Technische Fragen	
Welche LX-Modelle stehen zur Verfügung?	Zur Dominion LX-Produktfamilie gehören drei KVM-über-IP-Modelle. Der Switch DLX-108 verfügt über 8 Ports und unterstützt einen Remotebenutzer und einen lokalen Benutzer. Der Switch DLX-116 verfügt über 16 Ports und unterstützt einen Remotebenutzer und einen lokalen Benutzer. Der Switch DLX-216 verfügt über 16 Ports und unterstützt zwei Remotebenutzer und einen lokalen Benutzer.
Welche Hardwarefunktionen stehen zur Verfügung?	Der Dominion LX verfügt über ein kompaktes 1U-Gestell mit 8 bzw. 16 Serverports, Einzelstromversorgung, ein Gigabit-LAN sowie einen USB-basierten lokalen Port mit optionalem Modemzugriff.
Wie schneidet Dominion LX im Vergleich zum Dominion KX II ab?	Der Dominion KX II ist der beste und sichere KVM-über-IP-Switch der Unternehmensklasse von Raritan. Mit Modellen, die bis zu 64 Remoteserver und bis zu 8 Remotebenutzer unterstützen, eignet sich der KX II für Unternehmen und mittelständische Kunden, die Hunderte oder sogar Tausende Server verwalten. Der Dominion KX II ist branchenweit der zuverlässigste und sicherste Switch, der über zwei Netzteile, duales LAN, das Verschlüsselungsmodul FIPS 140-2 und Smart Card-/CAC-Authentifizierung verfügt. Bei Dominion LX handelt es sich um eine Reihe ökonomischer KVM-über-IP-Switches für kleine und mittelständische Unternehmen, die weniger als 75 Server verwalten müssen. Der LX ermöglicht Steuerung auf BIOS-Ebene und die IP-Steuerung von 8 bzw. 16 Servern mit Zugriffsmöglichkeiten für einen oder zwei Remotebenutzer.



Frage	Antwort
Welche Funktionen sind standardmäßig im Dominion LX enthalten?	Zu den standardmäßigen Funktionen von Dominion LX gehören: • Virtuelle Medien • Absolute Mouse Synchronization • Gängige browserbasierte Benutzeroberfläche für Remote- und lokalen Zugriff • Remote-Videoauflösung von 1920x1080 • Lokale und Remoteauthentifizierung (LDAP/AD/Radius) • Port- und Administratorberechtigungen • IPv6-/IPv4-Dual-Stack-Funktion • Port-Scanfunktion und Miniaturansichten • Schichtfunktion (Kaskadieren) mit anderen LX-Switches • Modemzugriff • Grundlegende Sicherheitsfunktionen Weitere Informationen finden Sie im Dokument **Dominion LX Features and Benefits** (Funktionen und Vorteile von Dominion LX).
Welche KX II-Funktionen sind im LX nicht verfügbar?	Folgende KX II-Funktionen sind im LX nicht verfügbar: • Zentrale Verwaltung CommandCenter® Secure Gateway (CC-SG) • Mobiler Zugriff über iPad® und iPhone® (CC-SG erforderlich) • Unterstützung für Bladeserver • Digitales Audio über IP • Verschlüsselungsmodul FIPS 140-2 • Smart Card-/CAC-Unterstützung • Sicherheitsmeldung bei Anmeldung • Integrierte Remotestromzufuhrsteuerung • Zwei Monitoroptionen und KVM-Client-Startoptionen
Welche CIMs (Serverdongle) kann LX einsetzen?	Der Dominion LX kann folgende CIMs verwenden: (1) die standardmäßigen Dominion CIMs und die Dominion CIMs für virtuelle Medien, (2) die ökonomischen MCUTP-Kabel-CIMs, und (3) die seriellen CIMs P2CIM-SER.
Was ist ein MCUTP-Kabel-CIM und welche Vorteile ergeben sich für mich?	Für Kunden, die nicht vorhaben, virtuelle Medien oder den Mausmodus "Absolute Mouse Synchronization" zu verwenden, sind MCUTP-Kabel-CIMs eine ökonomische Alternative zu Dominion CIMs. Das Kabel-CIM ist ein integriertes CIM und das Cat5-Kabel ist in unterschiedlichen Längen erhältlich.
Ermöglicht Dominion LX die zentrale Verwaltung?	Dominion LX verfügt standardmäßig nicht über die Funktion zur zentralen Verwaltung.

Frage	Antwort
Was sind virtuelle Medien?	Bei virtuellen Medien handelt es sich um eine leistungsstarke Funktion, mit der ein Benutzer während einer KVM-Verbindung Laufwerke und Medien von seinem Desktop auf Remoteservern installieren kann. Diese Funktion eignet sich besonders für Softwareinstallationen, die Durchführung von Hardwarediagnosen, die Dateiübertragung und sogar für die Erstellung eines neuen Serverabbilds von einem Remotestandort aus.
Welche Arten virtueller Medien unterstützt der Dominion LX?	Dominion LX unterstützt folgende virtuelle Medien: interne und per USB angeschlossene CD- und DVD-Laufwerke, USB-Massenspeichergeräte, PC-Festplatten und lokale sowie Remote-ISO-Abbilder.
Was ist "Absolute Mouse Synchronization"?	Es handelt sich um eine von Raritan entwickelte Technologie, bei der lokale und Remote-Cursor synchronisiert werden, ohne dass dafür eine Installation erforderlich ist. Dadurch erübrigt sich die mühsame manuelle Änderung der Mauseinstellungen auf den Zielservern.



Index

F

G

H

I

J

K

L



M

N

O

P

R

S

T

U

V

W



Z





USA/Kanada/Lateinamerika

Montag bis Freitag
08:00 bis 20:00 Uhr ET (Eastern Time)
Tel.: 800-724-8090 oder 732-764-8886
CommandCenter NOC: Drücken Sie auf Ihrem Telefon die Zifferntaste 6 und dann die Zifferntaste 1.
CommandCenter Secure Gateway: Drücken Sie auf Ihrem Telefon die Zifferntaste 6 und dann die Zifferntaste 2.
Fax: 732-764-8887
E-Mail-Adresse für CommandCenter NOC: tech-ccnoc@raritan.com
E-Mail-Adresse für alle anderen Produkte: tech@raritan.com

China

Peking

Montag bis Freitag
09:00 bis 18:00 Uhr Ortszeit
Tel.: +86-10-88091890

Shanghai

Montag bis Freitag
09:00 bis 18:00 Uhr Ortszeit
Tel.: +86-21-5425-2499

GuangZhou

Montag bis Freitag
09:00 bis 18:00 Uhr Ortszeit
Tel.: +86-20-8755-5561

Indien

Montag bis Freitag
09:00 bis 18:00 Uhr Ortszeit
Tel.: +91-124-410-7881

Japan

Montag bis Freitag
09:30 bis 17:30 Uhr Ortszeit
Tel.: +81-3-3523-5991
E-Mail: support.japan@raritan.com

Europa

Europa

Montag bis Freitag
08:30 bis 17:00 Uhr GMT+1 MEZ
Tel.: +31-10-2844040
E-Mail: tech.europe@raritan.com

Großbritannien

Montag bis Freitag
08:30 bis 17:00 Uhr GMT
Telefon +44(0)20-7090-1390

Frankreich

Montag bis Freitag
08:30 bis 17:00 Uhr GMT+1 MEZ
Tel.: +33-1-47-56-20-39

Deutschland

Montag bis Freitag
08:30 bis 17:30 Uhr GMT+1 MEZ
Tel.: +49-20-17-47-98-0
E-Mail: rg-support@raritan.com

Melbourne, Australien

Montag bis Freitag
09:00 bis 18:00 Uhr Ortszeit
Tel.: +61-3-9866-6887

Taiwan

Montag bis Freitag
09:00 bis 18:00 Uhr GMT -5 Standardzeit -4 Sommerzeit
Tel.: +886-2-8919-1333
E-Mail: support.apac@raritan.com